# TABLE OF CONTENTS

## INFORMATION SECURITY PROGRAM (PM)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PURPOSE</td>
<td>3</td>
</tr>
<tr>
<td>AUTHORITY</td>
<td>3</td>
</tr>
<tr>
<td>SCOPE AND APPLICABILITY</td>
<td>4</td>
</tr>
<tr>
<td>ORGANIZATION OF THE STATEWIDE INFORMATION SECURITY MANUAL</td>
<td>5</td>
</tr>
<tr>
<td>STATEWIDE INFORMATION SECURITY MANUAL CREATION AND MAINTENANCE</td>
<td>6</td>
</tr>
<tr>
<td>POLICY AND STANDARDS DISTRIBUTION</td>
<td>7</td>
</tr>
<tr>
<td>UPDATES</td>
<td>7</td>
</tr>
<tr>
<td>SECURITY COMMUNICATION AND TRAINING</td>
<td>7</td>
</tr>
<tr>
<td>ENFORCEMENT AND COMPLIANCE</td>
<td>7</td>
</tr>
<tr>
<td>QUESTIONS</td>
<td>8</td>
</tr>
</tbody>
</table>

## ORGANIZATIONAL SECURITY (OR)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR-01: POLICY</td>
<td>9</td>
</tr>
<tr>
<td>OR-02: INFORMATION SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES</td>
<td>9</td>
</tr>
<tr>
<td>OR-03: FUNCTIONAL ROLES AND RESPONSIBILITIES</td>
<td>16</td>
</tr>
<tr>
<td>OR-04: SEPARATION OF DUTIES</td>
<td>20</td>
</tr>
<tr>
<td>OR-05: CONTACTS WITH EXTERNAL ORGANIZATIONS</td>
<td>21</td>
</tr>
<tr>
<td>OR-06: INDEPENDENT REVIEW OF INFORMATION SECURITY PROGRAM</td>
<td>21</td>
</tr>
<tr>
<td>OR-07: REPORTING OF INCIDENTS</td>
<td>21</td>
</tr>
</tbody>
</table>

## COMPLIANCE (CP)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-01: POLICY</td>
<td>23</td>
</tr>
<tr>
<td>CP-02: SECURITY CONTROLS OVERSIGHT</td>
<td>23</td>
</tr>
<tr>
<td>CP-03: SECURITY ASSESSMENTS</td>
<td>24</td>
</tr>
<tr>
<td>CP-04: SECURITY ASSESSMENTS</td>
<td>FUNCTIONAL REVIEW OF SECURITY CONTROLS</td>
</tr>
<tr>
<td>CP-05: SECURITY ASSESSMENTS</td>
<td>INDEPENDENT ASSESSORS</td>
</tr>
<tr>
<td>CP-06: SECURITY ASSESSMENTS</td>
<td>OFFICE OF HOMELAND SECURITY AND PREPAREDNESS</td>
</tr>
<tr>
<td>CP-07: THIRD PARTY AUDITS</td>
<td>26</td>
</tr>
</tbody>
</table>

## PERSONNEL SECURITY (PS)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS-01: POLICY</td>
<td>27</td>
</tr>
<tr>
<td>PS-02: SECURITY REQUIREMENTS WITHIN POSITION DESCRIPTIONS</td>
<td>27</td>
</tr>
<tr>
<td>PS-03: WORKFORCE SCREENING</td>
<td>28</td>
</tr>
<tr>
<td>PS-04: RULES OF BEHAVIOR</td>
<td>29</td>
</tr>
<tr>
<td>PS-05: TRANSFERS AND PROMOTIONS</td>
<td>29</td>
</tr>
<tr>
<td>PS-06: PERSONNEL TERMINATION</td>
<td>30</td>
</tr>
<tr>
<td>PS-07: REPORTING OF INCIDENTS</td>
<td>30</td>
</tr>
<tr>
<td>SECURITY AWARENESS AND TRAINING (AW)</td>
<td>32</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----</td>
</tr>
<tr>
<td>AW-01: POLICY</td>
<td>32</td>
</tr>
<tr>
<td>AW-02: INFORMATION SECURITY AWARENESS PROGRAM</td>
<td>32</td>
</tr>
<tr>
<td>AW-03: INFORMATION SECURITY TRAINING</td>
<td>33</td>
</tr>
<tr>
<td>AW-04: ROLE-BASED SECURITY TRAINING</td>
<td>33</td>
</tr>
<tr>
<td>AW-05: INFORMATION SECURITY TRAINING RECORDS</td>
<td>34</td>
</tr>
<tr>
<td>AW-06: SECURITY ADVISORIES AND ALERTS</td>
<td>34</td>
</tr>
<tr>
<td>AW-07: INFORMATION SECURITY RESOURCES</td>
<td>34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RULES OF BEHAVIOR - ACCEPTABLE USE OF STATE INFORMATION ASSETS (RB)</th>
<th>35</th>
</tr>
</thead>
<tbody>
<tr>
<td>RB-01: POLICY</td>
<td>35</td>
</tr>
<tr>
<td>RB-02: AGENCY RESPONSIBILITY</td>
<td>35</td>
</tr>
<tr>
<td>RB-03: USER RESPONSIBILITIES</td>
<td>36</td>
</tr>
<tr>
<td>RB-04: ACCEPTABLE USE</td>
<td>36</td>
</tr>
<tr>
<td>RB-05: PROHIBITED USE</td>
<td>37</td>
</tr>
<tr>
<td>RB-06: NO EXPECTATION OF PRIVACY</td>
<td>38</td>
</tr>
<tr>
<td>RB-07: SECURITY MONITORING</td>
<td>38</td>
</tr>
<tr>
<td>RB-08: INCIDENTAL USE OF STATE OF NEW JERSEY INFORMATION ASSETS</td>
<td>39</td>
</tr>
<tr>
<td>RB-09: ADDITIONAL RULES FOR SECURITY AND PRIVILEGED ACCESS USERS</td>
<td>40</td>
</tr>
<tr>
<td>RB-10: VIOLATIONS</td>
<td>40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RISK MANAGEMENT (RM)</th>
<th>42</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM-01: POLICY</td>
<td>43</td>
</tr>
<tr>
<td>RM-02: RISK MANAGEMENT PROGRAM</td>
<td>43</td>
</tr>
<tr>
<td>RM-03: RISK-BASED SECURITY CATEGORIZATION</td>
<td>44</td>
</tr>
<tr>
<td>RM-04: RISK IDENTIFICATION</td>
<td>45</td>
</tr>
<tr>
<td>RM-05: RISK ASSESSMENTS</td>
<td>45</td>
</tr>
<tr>
<td>RM-06: RISK ASSESSMENT COMPONENTS</td>
<td>46</td>
</tr>
<tr>
<td>RM-07: RISK TREATMENT</td>
<td>47</td>
</tr>
<tr>
<td>RM-08: RISK ASSESSMENT UPDATES</td>
<td>47</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRIVACY (PR)</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR-01: POLICY</td>
<td>48</td>
</tr>
<tr>
<td>PR-02: GOVERNANCE AND PRIVACY PROGRAM</td>
<td>49</td>
</tr>
<tr>
<td>PR-03: PRIVACY IMPACT ASSESSMENT</td>
<td>49</td>
</tr>
<tr>
<td>PR-04: AUTHORITY TO COLLECT</td>
<td>50</td>
</tr>
<tr>
<td>PR-05: PRIVACY NOTICE</td>
<td>50</td>
</tr>
<tr>
<td>PR-06: CONSENT</td>
<td>50</td>
</tr>
<tr>
<td>PR-07: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION</td>
<td>51</td>
</tr>
<tr>
<td>PR-08: DATA QUALITY</td>
<td>51</td>
</tr>
<tr>
<td>PR-09: INTERNAL USE AND DISPLAY OF PERSONALLY IDENTIFIABLE INFORMATION</td>
<td>51</td>
</tr>
<tr>
<td>PR-10: PRINCIPLE OF LEAST PRIVILEGE</td>
<td>52</td>
</tr>
<tr>
<td>PR-11: INDIVIDUAL ACCESS</td>
<td>52</td>
</tr>
<tr>
<td>PR-12: REDRESS</td>
<td>53</td>
</tr>
<tr>
<td>PR-13: USER FEEDBACK MANAGEMENT</td>
<td>53</td>
</tr>
<tr>
<td>PR-14: INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION</td>
<td>53</td>
</tr>
<tr>
<td>PR-15: INFORMATION SHARING</td>
<td>54</td>
</tr>
<tr>
<td>PR-16: PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS</td>
<td>54</td>
</tr>
<tr>
<td>PR-17: PRIVACY INCIDENT RESPONSE</td>
<td>54</td>
</tr>
<tr>
<td>PR-18: PRIVACY AWARENESS AND TRAINING</td>
<td>55</td>
</tr>
<tr>
<td>PR-19: DATA RETENTION AND DISPOSAL</td>
<td>55</td>
</tr>
</tbody>
</table>

| INFORMATION ASSET MANAGEMENT (AM)                 | 57 |
| AM-01: POLICY                                     | 58 |
| AM-02: INFORMATION ASSET IDENTIFICATION AND INVENTORY | 58 |
| AM-03: UPDATES DURING INSTALLATIONS, REMOVALS, UPDATES, AND MAINTENANCE | 59 |
| AM-04: AUTOMATED UNAUTHORIZED COMPONENT DETECTION  | 59 |
| AM-05: NETWORK ACCESS CONTROL (NAC)               | 59 |
| AM-06: DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING | 59 |
| AM-07: SOFTWARE LICENSING RESTRICTIONS            | 59 |
| AM-08: ASSIGNING CUSTODIANSHIP OF ASSETS          | 60 |
| AM-09: ACCEPTABLE USE OF STATE INFORMATION ASSETS | 60 |
| AM-10: RETURN OF ASSETS                           | 60 |
| AM-11: REMOVAL OF ASSETS                          | 61 |
| AM-12: USE OF PERSONAL DEVICES                    | 61 |
| AM-13: USE OF THIRD-PARTY DEVICES                 | 61 |

| SECURITY CATEGORIZATION (SC)                      | 63 |
| SC-01: POLICY                                     | 64 |
| SC-02: SECURITY CATEGORIZATIONS                   | 64 |
| SC-03: ASSIGNING SECURITY CATEGORIZATIONS         | 65 |
| SC-04: RISK CONSIDERATIONS                        | 66 |
| SC-05: LABELING                                   | 66 |

| MEDIA PROTECTION (MP)                             | 69 |
| MP-01: POLICY                                     | 70 |
| MP-02: SECURITY CATEGORIZATION                    | 70 |
| MP-03: MEDIA STORAGE                              | 71 |
| MP-04: SENSITIVE DATA INVENTORIES                 | 71 |
| MP-05: CRYPTOGRAPHIC PROTECTION                   | 71 |
| MP-06: MEDIA ACCESS                               | 72 |
| MP-07: PORTABLE STORAGE DEVICES                   | 72 |
| MP-08: MEDIA TRANSPORTATION                       | 73 |
| MP-09: DATA LOSS PREVENTION                       | 74 |
| MP-10: MEDIA SANITIZATION                         | 74 |
| MP-11: RECORDS RETENTION                          | 75 |
CRYPTOGRAPHIC PROTECTION (CR)

CR-01: POLICY
CR-02: USE OF CRYPTOGRAPHIC CONTROLS
CR-03: ENCRYPTION ALGORITHMS
CR-04: ENCRYPTION OF DATA IN TRANSIT
CR-05: ENCRYPTION OF DATA AT REST
CR-06: CRYPTOGRAPHIC PROTECTION FOR AUTHENTICATORS
CR-07: NON-CONSOLE ADMINISTRATIVE ACCESS
CR-08: WIRELESS ACCESS AUTHENTICATION AND ENCRYPTION
CR-09: CRYPTOGRAPHIC KEY MANAGEMENT
CR-10: SYMMETRIC AND ASYMMETRIC KEYS

ACCESS MANAGEMENT (AC)

AC-01: POLICY
AC-02: ROLE BASED ACCESS
AC-03: PRINCIPLE OF LEAST PRIVILEGE
AC-04: SEGREGATION OF DUTIES
AC-05: USER ACCOUNT MANAGEMENT
AC-06: REQUIREMENTS FOR ACCOUNT REGISTRATION AND CREATION
AC-07: REQUIREMENTS FOR PRIVILEGED ACCESS
AC-08: REQUIREMENTS FOR TEMPORARY OR EMERGENCY ACCESS
AC-09: USER ACCOUNT LOCK OUT AND SUSPENSION
AC-10: SESSION LOCK
AC-11: MANAGEMENT OF USER ACCOUNTS AND ACCESS
AC-12: SUSPENSION OF ACTIVE ACCOUNTS
AC-13: SYSTEM USE NOTIFICATION
AC-14: PERIODIC REVIEW

IDENTITY AND AUTHENTICATION (IA)

IA-01: POLICY
IA-02: PRINCIPLE OF LEAST PRIVILEGE
IA-03: IDENTIFICATION AND AUTHENTICATION
IA-04: USER PROVISIONING AND DEPROVISIONING
IA-05: ROLE BASED ACCESS CONTROL
IA-06: USER ACCOUNT MANAGEMENT
IA-07: IDENTIFIER MANAGEMENT
IA-08: AUTHENTICATOR MANAGEMENT
IA-09: MULTI-FACTOR AUTHENTICATION (MFA)
IA-10: MULTI-FACTOR AUTHENTICATION – SEPARATE DEVICE
IA-11: PASSWORD AUTHENTICATION MANAGEMENT
IA-12: PASSWORD REQUIREMENTS FOR STANDARD USER ACCOUNTS
IA-13: PASSWORD REQUIREMENTS FOR ADMINISTRATIVE ACCOUNTS 100
IA-14: PASSWORD REQUIREMENTS FOR SERVICE ACCOUNTS 101
IA-15: PASSWORD REQUIREMENTS FOR PUBLICLY-FACING WEB APPLICATIONS 102
IA-16: RESTRICTIONS ON DISPLAYING PASSWORDS 103
IA-17: SESSION LOCK 103
IA-18: PKI-BASED AUTHENTICATION 103
IA-19: PERIODIC REVIEW 103

REMOTE ACCESS (RA) 105
RA-01: POLICY 106
RA-02: CENTRALIZED MANAGEMENT OF REMOTE ACCESS INFRASTRUCTURE 106
RA-03: REMOTE ACCESS SECURITY 107
RA-04: AGENCY LEVEL AUTHORIZATION 109
RA-05: TRAINING OF REMOTE ACCESS USERS 109
RA-06: REMOTE ACCESS USER RESPONSIBILITIES 110

SECURITY ENGINEERING AND ARCHITECTURE (SE) 111
SE-01: POLICY 111
SE-02: SECURITY ENGINEERING PRINCIPLES 111
SE-03: ALIGNMENT WITH ENTERPRISE ARCHITECTURE 112
SE-04: SECURE CONFIGURATIONS 113
SE-05: LEAST PRIVILEGE 114
SE-06: SECURITY FUNCTION ISOLATION 115
SE-07: DEFENSE IN-DEPTH 115
SE-08: APPLICATION PARTITIONING 116
SE-09: SYSTEM PARTITIONING 116
SE-10: FIREWALL AND ROUTER CONFIGURATIONS 117
SE-11: SECURE LOG-ON 117
SE-12: PREVIOUS LOGON NOTIFICATION 118
SE-13: LOGON BANNER 118
SE-14: FAIL SECURE IN KNOWN STATE 119
SE-15: FAIL-SAFE PROCEDURES 119
SE-16: CLOCK SYNCHRONIZATION 119

CONFIGURATION MANAGEMENT (CM) 121
CM-01: POLICY 121
CM-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS 121
CM-03: AUTOMATED CENTRAL MANAGEMENT AND VERIFICATION OF BASELINE CONFIGURATIONS 122
CM-04: LEAST FUNCTIONALITY 123
CM-05: SOFTWARE USAGE RESTRICTIONS 124
ENDPOINT SECURITY (ES) 125
ES-01: POLICY 125
ES-02: INVENTORY OF ENDPOINT DEVICES 125
ES-03: SECURITY CATEGORIZATION OF ENDPOINT 125
ES-04: SOFTWARE CURRENCY 126
ES-05: ACCESS CONTROLS 126
ES-06: SESSION LOCK 126
ES-07: DATA PROTECTION MEASURES 126
ES-08: PROTECTION AGAINST MALICIOUS CODE 127
ES-09: FILE INTEGRITY MONITORING (FIM) 127
ES-10: HOST-BASED FIREWALL 128
ES-11: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS/HIPS) 128
ES-12: MOBILE CODE SECURITY 129
ES-13: TRUSTED PATH 129
ES-14: HYPervisor ACCESS 130
ES-15: PORT AND I/O DEVICE ACCESS 130
ES-16: AUDIT LOGGING 130

EMBEDDED SYSTEMS (EM) 132
EM-01: POLICY 133
EM-02: EMBEDDED TECHNOLOGY SECURITY 133
EM-03: INTERNET OF THINGS (IOT) 134
EM-04: OPERATIONAL TECHNOLOGY (OT) 134

MOBILE DEVICE MANAGEMENT (MD) 135
MD-01: POLICY 136
MD-02: AUTHORIZATION FOR USE OF MOBILE DEVICES 136
MD-03: RISK ASSESSMENT 137
MD-04: BRING YOUR OWN DEVICE (BYOD) 137
MD-05: NETWORK ACCESS 138
MD-06: CENTRALIZED MANAGEMENT 138
MD-07: ELIGIBLE MOBILE DEVICES 139
MD-08: TECHNICAL SECURITY CONTROLS 139
MD-09: INVENTORY 141
MD-10: APPROVED APPLICATION STORES 141
MD-11: APPROVED APPLICATIONS 141
MD-12: APPLICATION MANAGEMENT 142
MD-13: APPROVED CLOUD SERVICES 142
MD-14: BACKUP 142
MD-15: SAFETY AND COMPLIANCE 142
MD-16: TRAINING OF MOBILE DEVICE USERS 142
<table>
<thead>
<tr>
<th>NETWORK SECURITY (NS)</th>
<th>144</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS-01: POLICY</td>
<td>144</td>
</tr>
<tr>
<td>NS-02: NETWORK MANAGEMENT</td>
<td>144</td>
</tr>
<tr>
<td>NS-03: IDENTIFIED RESPONSIBILITY</td>
<td>145</td>
</tr>
<tr>
<td>NS-04: DOCUMENTATION</td>
<td>145</td>
</tr>
<tr>
<td>NS-05: GENERAL PHYSICAL SECURITY REQUIREMENTS</td>
<td>146</td>
</tr>
<tr>
<td>NS-06: LAYERED DEFENSES</td>
<td>146</td>
</tr>
<tr>
<td>NS-07: BOUNDARY PROTECTION</td>
<td>148</td>
</tr>
<tr>
<td>NS-08: DATA FLOW ENFORCEMENT - ACCESS CONTROL lists (ACLS)</td>
<td>150</td>
</tr>
<tr>
<td>NS-09: INFORMATION SYSTEM CONNECTIONS</td>
<td>151</td>
</tr>
<tr>
<td>NS-10: SECURITY FUNCTION ISOLATION</td>
<td>153</td>
</tr>
<tr>
<td>NS-11: NETWORK DISCONNECT/TIMEOUT</td>
<td>154</td>
</tr>
<tr>
<td>NS-12: NETWORK INTRUSION DETECTION &amp; PREVENTION SYSTEMS (NIDS/NIPS)</td>
<td>154</td>
</tr>
<tr>
<td>NS-13: SAFEGUARDING DATA OVER OPEN NETWORKS</td>
<td>155</td>
</tr>
<tr>
<td>NS-14: REMOTE ACCESS</td>
<td>156</td>
</tr>
<tr>
<td>NS-15: DOMAIN NAME SERVICE (DNS) RESOLUTION</td>
<td>157</td>
</tr>
<tr>
<td>NS-16: WIRELESS NETWORKING</td>
<td>158</td>
</tr>
<tr>
<td>NS-17: DATA LOSS PREVENTION (DLP)</td>
<td>159</td>
</tr>
<tr>
<td>NS-18: INTERNET PROXY</td>
<td>160</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLOUD SECURITY (CL)</th>
<th>162</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL-01: POLICY</td>
<td>163</td>
</tr>
<tr>
<td>CL-02: CLOUD ACQUISITION AND DEVELOPMENT</td>
<td>164</td>
</tr>
<tr>
<td>CL-03: CLOUD PROVIDERS</td>
<td>164</td>
</tr>
<tr>
<td>CL-04: CLOUD SECURITY ARCHITECTURE</td>
<td>165</td>
</tr>
<tr>
<td>CL-05: SECURITY MANAGEMENT SUBNET</td>
<td>166</td>
</tr>
<tr>
<td>CL-06: APPLICATION PROGRAM INTERFACE (API) SECURITY</td>
<td>166</td>
</tr>
<tr>
<td>CL-07: SECURITY ROLES AND RESPONSIBILITIES</td>
<td>166</td>
</tr>
<tr>
<td>CL-08: VIRTUAL MACHINE IMAGES</td>
<td>166</td>
</tr>
<tr>
<td>CL-09: MULTI-TENANT ENVIRONMENTS</td>
<td>167</td>
</tr>
<tr>
<td>CL-10: DATA HANDLING AND PORTABILITY</td>
<td>167</td>
</tr>
<tr>
<td>CL-11: STANDARDIZED VIRTUALIZATION FORMATS</td>
<td>167</td>
</tr>
<tr>
<td>CL-12: MOBILE DEVICE ACCESS</td>
<td>167</td>
</tr>
<tr>
<td>CL-13: GEOLOCATION REQUIREMENTS</td>
<td>168</td>
</tr>
<tr>
<td>CL-14: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS</td>
<td>168</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHANGE MANAGEMENT (CH)</th>
<th>170</th>
</tr>
</thead>
<tbody>
<tr>
<td>CH-01: POLICY</td>
<td>170</td>
</tr>
<tr>
<td>CH-02: CONFIGURATION CHANGE CONTROL</td>
<td>170</td>
</tr>
<tr>
<td>CH-03: STAKEHOLDER NOTIFICATION OF CHANGES</td>
<td>171</td>
</tr>
<tr>
<td>CH-04: SECURITY IMPACT ANALYSIS FOR CHANGES</td>
<td>171</td>
</tr>
<tr>
<td>CH-05: SECURITY FUNCTIONALITY VERIFICATION</td>
<td>171</td>
</tr>
<tr>
<td>INFORMATION ASSET MAINTENANCE (MA)</td>
<td>173</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>MA-01: POLICY</td>
<td>173</td>
</tr>
<tr>
<td>MA-02: MAINTENANCE OPERATIONS</td>
<td>173</td>
</tr>
<tr>
<td>MA-03: CONTROLLED MAINTENANCE</td>
<td>173</td>
</tr>
<tr>
<td>MA-04: TIMELY MAINTENANCE</td>
<td>174</td>
</tr>
<tr>
<td>MA-05: REMOTE MAINTENANCE</td>
<td>174</td>
</tr>
<tr>
<td>MA-06: MAINTENANCE PERSONNEL</td>
<td>175</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT MANAGEMENT (TM)</th>
<th>176</th>
</tr>
</thead>
<tbody>
<tr>
<td>TM-01: POLICY</td>
<td>176</td>
</tr>
<tr>
<td>TM-02: THREAT AWARENESS PROGRAM</td>
<td>176</td>
</tr>
<tr>
<td>TM-03: THREAT INTELLIGENCE</td>
<td>177</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VULNERABILITY AND PATCH MANAGEMENT (VU)</th>
<th>178</th>
</tr>
</thead>
<tbody>
<tr>
<td>VU-01: POLICY</td>
<td>178</td>
</tr>
<tr>
<td>VU-02: VULNERABILITY AND PATCH MANAGEMENT PROGRAM</td>
<td>178</td>
</tr>
<tr>
<td>VU-03: VULNERABILITY SCANNING</td>
<td>179</td>
</tr>
<tr>
<td>VU-04: VULNERABILITY RANKING</td>
<td>180</td>
</tr>
<tr>
<td>VU-05: VULNERABILITY REMEDIATION PROCESS</td>
<td>180</td>
</tr>
<tr>
<td>VU-06: VULNERABILITY REMEDIATION</td>
<td>180</td>
</tr>
<tr>
<td>VU-07: SOFTWARE PATCHING</td>
<td>181</td>
</tr>
<tr>
<td>VU-08: PENETRATION TESTING</td>
<td>181</td>
</tr>
<tr>
<td>VU-09: INDEPENDENT PENETRATION TESTING</td>
<td>182</td>
</tr>
<tr>
<td>VU-10: RED TEAM EXERCISES</td>
<td>182</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTINUOUS MONITORING (CO)</th>
<th>184</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO-01: POLICY</td>
<td>185</td>
</tr>
<tr>
<td>CO-02: CONTINUOUS MONITORING</td>
<td>185</td>
</tr>
<tr>
<td>CO-03: CENTRALIZED EVENT LOG COLLECTION</td>
<td>187</td>
</tr>
<tr>
<td>CO-04: CONTENT OF AUDIT RECORDS</td>
<td>188</td>
</tr>
<tr>
<td>CO-05: PROTECTION OF AUDIT RECORDS</td>
<td>189</td>
</tr>
<tr>
<td>CO-06: REPORTING</td>
<td>190</td>
</tr>
<tr>
<td>CO-07: CLOCK SYNCHRONIZATION</td>
<td>190</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY IN SOFTWARE DEVELOPMENT (SD)</th>
<th>191</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-01: POLICY</td>
<td>191</td>
</tr>
<tr>
<td>SD-02: SECURE DEVELOPMENT</td>
<td>191</td>
</tr>
<tr>
<td>SD-03: SECURE CODING</td>
<td>192</td>
</tr>
<tr>
<td>SD-04: SEPARATION OF DEVELOPMENT, TESTING &amp; OPERATIONAL ENVIRONMENTS</td>
<td>192</td>
</tr>
<tr>
<td>SD-05: INFORMATION INPUT RESTRICTIONS</td>
<td>193</td>
</tr>
<tr>
<td>SD-06: INPUT DATA VALIDATION</td>
<td>193</td>
</tr>
<tr>
<td>SD-07: ERROR HANDLING</td>
<td>193</td>
</tr>
<tr>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td></td>
</tr>
<tr>
<td>SD-08: SECURITY TESTING THROUGHOUT DEVELOPMENT</td>
<td>194</td>
</tr>
<tr>
<td>SD-09: USE OF LIVE DATA</td>
<td>195</td>
</tr>
<tr>
<td>SD-10: ACCESS TO PROGRAM SOURCE CODE</td>
<td>195</td>
</tr>
<tr>
<td>SD-11: TRAINING</td>
<td>195</td>
</tr>
</tbody>
</table>

| SECURITY FOR PUBLICLY-ACCESSIBLE WEBSITES AND SERVICES (WS) | 196 |
| WS-01: POLICY | 196 |
| WS-02: HTTPS-ONLY | 196 |
| WS-03: USE OF DEMILITARIZED ZONES (DMZ) | 198 |
| WS-04: WEB APPLICATION FIREWALL (WAF) | 198 |
| WS-05: ACCESS CONTROLS FOR PUBLICLY-FACING WEB APPLICATIONS | 199 |
| WS-06: PRIVACY | 199 |
| WS-07: APPROVED DOMAINS | 200 |
| WS-08: PUBLICLY ACCESSIBLE CONTENT | 200 |

| PROJECT AND RESOURCE MANAGEMENT (PM) | 202 |
| PM-01: POLICY | 202 |
| PM-02: ALLOCATION OF RESOURCES | 202 |
| PM-03: SECURITY REQUIREMENTS DEFINITION | 203 |
| PM-04: SECURITY IN PROJECT MANAGEMENT | 203 |
| PM-05: SYSTEM SECURITY PLAN | 203 |
| PM-06: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) | 203 |

| CAPACITY AND PERFORMANCE PLANNING (CA) | 205 |
| CA-01: POLICY | 205 |
| CA-02: CAPACITY MANAGEMENT | 205 |
| CA-03: RESOURCE PRIORITY | 205 |

| THIRD PARTY MANAGEMENT (TP) | 207 |
| TP-01: POLICY | 208 |
| TP-02: THIRD PARTY RISK ASSESSMENTS | 208 |
| TP-03: CONTRACT REQUIREMENTS | 208 |
| TP-04: THIRD-PARTY INTERCONNECTIONS | 209 |
| TP-05: THIRD PARTY MANAGEMENT | 211 |
| TP-06: THIRD PARTY PERSONNEL SECURITY | 212 |
| TP-07: SUPPLY CHAIN PROTECTION | 212 |
| TP-08: TRUSTWORTHINESS | 213 |

| SECURITY ASSESSMENT AND AUTHORIZATION (SA) | 214 |
| SA-01: POLICY | 215 |
| SA-02: SECURITY CATEGORIZATION | 215 |
| SA-03: PRIVACY IMPACT ASSESSMENT | 216 |
| SA-04: SYSTEM SECURITY PLAN | 216 |
SA-05: SECURITY ASSESSMENT
SA-06: AUTHORITY TO OPERATE
SA-07: CONTINUOUS MONITORING REQUIREMENT

EXCEPTION MANAGEMENT (EX)
EX-01: POLICY
EX-02: EXCEPTION REQUEST SUBMISSIONS
EX-03: EXCEPTION REQUEST REQUIREMENTS
EX-04: REQUEST DETERMINATIONS
EX-05: PERIODIC REVIEW

PHYSICAL AND ENVIRONMENTAL SECURITY (PE)
PE-01: POLICY
PE-02: PHYSICAL ACCESS SECURITY ZONES
PE-03: PHYSICAL ACCESS AUTHORIZATION
PE-04: VISITOR CONTROL
PE-05: LOST OR STOLEN ID BADGES
PE-06: PHYSICAL ACCESS CONTROLS
PE-07: SECURITY MONITORING AND AUDITING OF PHYSICAL ACCESS
PE-08: RETENTION OF SECURITY LOGS AND VIDEO
PE-09: LOCATION OF INFORMATION ASSETS
PE-10: CLEAN DESK/CLEAN SCREEN REQUIREMENTS
PE-11: POWER EQUIPMENT AND POWER CABLING
PE-12: EMERGENCY SHUTOFF
PE-13: EMERGENCY POWER
PE-14: EMERGENCY LIGHTING
PE-15: FIRE PROTECTION
PE-16: TEMPERATURE AND HUMIDITY CONTROLS
PE-17: WATER DAMAGE PROTECTION
PE-18: DELIVERY AND REMOVAL OF INFORMATION ASSETS
PE-19: SECURING PORTABLE INFORMATION ASSETS
PE-20: DISPOSAL/TRANSFER OF INFORMATION ASSETS

CONTINGENCY PLANNING (CT)
CT-01: POLICY
CT-02: CONTINGENCY PLAN
CT-03: MANAGEMENT OF CONTINGENCY PLANS
CT-04: CONTINGENCY PLAN TESTING AND EXERCISES
CT-05: CONTINGENCY TRAINING
CT-06: ALTERNATE SITE
CT-07: INFORMATION SYSTEM BACKUP
CT-08: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CT-09: CONTINGENCY PLAN ROOT CAUSE ANALYSIS
CT-10: CONTINGENCY PLAN UPDATE

<table>
<thead>
<tr>
<th>INCIDENT RESPONSE (IR)</th>
<th>236</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-01: POLICY</td>
<td>236</td>
</tr>
<tr>
<td>IR-02: REPORTING INFORMATION SECURITY INCIDENTS</td>
<td>236</td>
</tr>
<tr>
<td>IR-03: INCIDENT RESPONSE PLANNING</td>
<td>237</td>
</tr>
<tr>
<td>IR-04: INCIDENT RESPONSE TEAM</td>
<td>237</td>
</tr>
<tr>
<td>IR-05: INCIDENT CATEGORIZATION</td>
<td>239</td>
</tr>
<tr>
<td>IR-06: INCIDENT SEVERITY AND PRIORITIZATION</td>
<td>241</td>
</tr>
<tr>
<td>IR-07: INCIDENT TRACKING, DOCUMENTATION AND REPORTS</td>
<td>241</td>
</tr>
</tbody>
</table>

APPENDIX A – SECURITY CATEGORIZATION CONSIDERATIONS | 243

APPENDIX B – GLOSSARY OF KEY TERMS | 247

APPENDIX C – RECORD OF CHANGES | 361
The State of New Jersey affirms the fundamental significance of information security by delineating a set of policies and standards to securely protect the Executive Branch of New Jersey State Government information and information systems, while maintaining compliance with State and Federal laws, executive orders, regulatory, contractual, and other policy requirements pertaining to confidentiality, integrity, availability, privacy, and safety. New Jersey State Government departments and agencies act as the custodians of extensive information holdings and rely upon information systems for fiscal, policy, and program delivery initiatives. Consequently, security measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of information and information systems, and safeguards must be implemented to offset possible threats.

The information security policies, standards, processes, and guidelines contained in the Statewide Information Security Manual are key components of the State’s information security program. Five information security objectives: Confidentiality, Integrity, Availability, Privacy, and Safety comprise its foundation.

- **Confidentiality** – The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
- **Integrity** - The property that sensitive information has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** - The property of information or an information system being accessible and useable upon demand by an authorized entity.
- **Privacy** - Freedom from unauthorized intrusion or disclosure of information about an individual.
- **Safety** - The condition of being protected from harm or other non-desirable outcomes.
These information security objectives can only be achieved if organizations embed them into their people, processes, and technology.

- **People** – Everyone has a role to play in information security. Security is implemented and practiced by people. People design and implement processes and technology, as well as follow processes and use technology to enable business.

- **Process** - includes formal and informal mechanisms (large and small, simple and complex) to get things. Processes identify, measure, manage, and control risks to confidentiality, integrity, availability, privacy, and safety, and they also ensure accountability.

- **Technology** - is composed of all of the tools, applications, and infrastructure that make processes more efficient. Technology implemented by people following processes allows for the State to meet its information security objectives.
PURPOSE

The purpose of the Executive Branch of New Jersey State Government’s Statewide Information Security Manual, hereinafter referred to as the Manual, is to assist New Jersey State Government organizations in applying a risk–based approach to information security while establishing the required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy and maintain the physical safety of individuals.

This Manual includes a set of policies, standards, procedures, and guidelines that sets a clear direction for information security and its role in supporting Executive Branch departments and agencies in their efforts to carry out their respective missions and to achieve their business goals and objectives, while effectively managing risk and ensuring the confidentiality, integrity and availability of their information and information systems. This Manual provides direction to the State workforce regarding their roles and responsibilities with respect to the security of State information assets. The implementation of consistent security controls across the Executive Branch of New Jersey State Government will help departments and agencies comply with current and future legal obligations to ensure due diligence in protecting the confidentiality, integrity, availability, and privacy of State information and information systems.

The Executive Branch of New Jersey State Government’s Statewide Information Security Manual has been derived from applicable State and federal laws; industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; the Center for Internet Security (CIS) Top 20 Critical Security Controls; the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); lessons learned; and other New Jersey State Government business and technology related considerations.

This Manual is intended to provide State agencies with a means to tailor cost-effective security controls necessary to protect the confidentiality, integrity, availability, and privacy of State information and information systems commensurate with their sensitivity and criticality, while also maintaining and ensuring compliance with all legal requirements.

AUTHORITY

The policies, standards, and guidelines included in the Executive Branch of New Jersey State Government’s Statewide Information Security Manual are established under the authority of:

- New Jersey Executive Order No. 5 creating the Office of Homeland Security and Preparedness (OHSP) (Corzine, 3/6/2006);
- New Jersey Executive Order No. 178 creating the New Jersey Cybersecurity and Communications Integration Cell (“NJCCIC”) (Christie, 5/20/2015);
The Critical Infrastructure Information Act of 2002, 6 U.S.C. § 133 et seq.; and


The Information Security Policies and Standards are supported at the highest levels of the Executive Branch of New Jersey State Government.

**SCOPE AND APPLICABILITY**

The policies, standards, procedures, and guidelines included in the Statewide Information Security Manual apply to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of New Jersey State Government, hereinafter referred to as: agencies, the Executive Branch, the SoNJ, or the State. All Executive Branch full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities - collectively referred to as users are governed by and responsible for complying with the policies and standards regardless of agency, location, or role.

This Manual applies to all information assets owned, leased, licensed, managed, or used by Executive Branch agencies, their business partners, contractors, or other authorized third-parties on behalf of the State of New Jersey. Information assets include but are not limited to all information, data, devices, hardware (e.g. servers, laptop and desktop computers, tablets, phones, switches, etc.), software (e.g. commercial off-the-shelf and custom developed applications and support systems), services, or other components of information or communications systems.

The policies, standards, procedures, and guidelines included in this Manual supersede any previous Executive Branch Statewide information security policies, standards, procedures, and guidelines issued prior to March 5, 2018, the effective date. These policies, standards, procedures, and guidelines have been written in conformance with and do not supersede any applicable State or Federal laws, Executive Orders, or existing contracts, memorandum of understanding, or labor management agreements in effect as of the effective date of the Statewide Information Security Manual.

Executive Branch agencies are required to abide by the policies and standards documented herein. Agencies may develop and implement a more restrictive set of information security policies and standards for use within their respective organization or for a specific information system, program, or requirement. Agency-developed information security policies and standards can exceed, but must not conflict with, the baseline established by this Manual.

The Executive Branch of New Jersey State Government’s Statewide Information Security Manual does not apply to independent State entities that are not subject to the policy supervision and control of the Governor. Examples of independent State entities include the New Jersey Transit Authority, the New Jersey Turnpike Authority, etc.
ORGANIZATION OF THE STATEWIDE INFORMATION SECURITY MANUAL

The individual information security policies, standards, procedures, and guidelines, along with their supporting references and forms, have been compiled and organized into the Executive Branch of New Jersey State Government’s Statewide Information Security Manual as each policy, standard, and guideline presented has key dependencies with others. The collection of policies, standards, procedures, and guidelines organized as a whole within this Manual provides context, consistency, and clarity, whereas separate policies and standards may lead to gaps, inconsistencies, and conflicts.

Information security documentation is comprised of four (4) main parts: core policies; standards that are mandatory controls used to support a policy; procedures that contain the steps necessary to implement a policy; and guidelines that are recommended approaches to implementing a policy. When applied in concert they allow for security objectives to be met.

- **Policy** - Documents high-level rules, establishes roles and responsibilities, and sets management expectations governing security practices, operational procedures, and the acceptable use of State information assets. Policies are supported by standards and further implemented by procedures.

- **Standard** - A mandatory control that helps enforce and support a policy. Standards include specifications for processes, practices, uses, and hardware and software configurations that are considered industry or government approved specifications. External standards organizations, such as the National Institute of Standards and Technology, the Cloud Security Alliance, the Center for Internet Security, and others publish approved information security standards that are included in this Manual.

- **Procedure** - Contains detailed descriptions of the steps necessary to perform specific operations in conformance with applicable standards and represent the implementation of a policy. They are generally developed by those who are responsible for the implementation of a policy or standard, such as systems administrators, network administrators, database administrators, etc.

- **Guideline** - Consists of recommendations, best practices, or support documents and processes that help with the interpretation and implementation of a specific policy or standard. Guidelines are intended to help agencies and individuals to achieve a policy's objectives by providing a framework within which to implement procedures while allowing for discretion in their interpretation, implementation, or use. They include background information regarding the policy, standards, and control objectives. Guidelines may also provide a description of a particular way of accomplishing something that is less prescriptive than a procedure.
The State Chief Information Security Officer (CISO), within the Office of Homeland Security and Preparedness’ Division of Cybersecurity, has overall responsibility for the creation and maintenance of the Executive Branch of New Jersey State Government’s Statewide Information Security Manual.

The policies, standards, procedures, and guidelines contained in this Manual shall be reviewed and approved at least annually by the CISO, under the oversight of the Information Security Governance Committee, to ensure the State’s security program is relevant and applicable to manage the risks associated with new and emerging security threats and vulnerabilities as they arise.

Reviews of the Manual must also be initiated under the following circumstances:

(a) In conjunction with legislative, regulatory, or policy changes that have information security implications;

(b) To account for the planning and implementation of new or significantly changed technologies;

(c) In response to a security risk assessment or audit in which the current controls are deemed to expose the State to unacceptable risks;

(d) In response to threat or vulnerability trends that indicate State information and information systems are at significantly increased risk;

(e) After the review of a significant information security incident; and/or

(f) When industry, national, or international standards for information security are introduced or significantly revised to address emerging business and technology issues.

The Manual is considered a living document and, as such, is subject to changes and modifications, with or without notification, as necessary to protect the State’s business objectives, individuals,
and assets. The State reserves the right to revoke, change, or supplement these policies, standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by the State CISO, unless otherwise stated.

**POLICY AND STANDARDS DISTRIBUTION**

The State CISO is responsible for the creation and distribution of the Statewide Information Security Manual to all agencies. At a minimum, the contents of the Manual shall be distributed for viewing on agency Intranet websites.

**UPDATES**

Substantive changes or updates to the Manual will be announced to employees via email and/or announced on the OHSP Division of Cybersecurity website. Changes will be noted in the Record of Changes.

**SECURITY COMMUNICATION AND TRAINING**

Executive Branch agencies shall ensure that all users are familiar with the requirements of the Executive Branch of New Jersey State Government’s Statewide Information Security Manual. Agencies shall conduct security awareness training for all users at least annually, to ensure that all personnel are aware of the security risks associated with their roles and that they understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of State information systems and information. New hires are required to complete information security awareness training within thirty (30) business days of their start date, as part of the required new hire training curriculum.

Agencies shall ensure that all interns, temporary workers, and contracted third parties covered by the Manual are familiar with it and comply with its requirements.

Users will be kept abreast of policy and standard changes via the following communication methods:

- Emails;
- State Internet sites;
- Department and Agency Intranet sites;
- Staff meetings;
- Annual security awareness training; and/or
- Other communications mediums as required.

**ENFORCEMENT AND COMPLIANCE**

All users of Executive Branch of New Jersey State Government information and information systems are governed by, and are responsible for, complying with the information security policies and standards. Users who are found in violation of the information security policies and
standards are subject to disciplinary action up to and including termination of employment, or immediate termination of contractor and/or vendor relationship. Violations of law may be referred to the appropriate law enforcement agency for investigation and prosecution.

**QUESTIONS**
Questions about this Manual may be directed to your respective Agency Chief Information Security Officer or to the Office of Homeland Security and Preparedness’ Division of Cybersecurity, via email at security@cyber.nj.gov.

**REFERENCES**
The requirements established in the Information Security Charter have been derived from the following:

- NIST SP 800-53 Program Management (PM); and
- NIST CSF Identify/Governance (ID.GV).
ORGANIZATIONAL SECURITY (OR)

PURPOSE
The purpose of the Organizational Security Policy is to establish and maintain a management framework that promotes and oversees the implementation of security controls and the performance of information security throughout the Executive Branch of New Jersey State Government.

KEY TERMS
None. See Glossary in Appendix B for complete listing of terms.

OR-01: POLICY
The Chief Technology Officer (CTO) of New Jersey and the Director, New Jersey Office of Homeland Security and Preparedness (NJOHSP) jointly establish the Information Security Governance Committee and a management structure for information security across the Executive Branch of New Jersey State Government.

This policy incorporates the requirements from the State of New Jersey Office of Information Technology Circular, Enterprise Information Security Governance and Management Policy, 17-03-NJOIT.

OR-02: INFORMATION SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES
The primary roles within the Executive Branch of the New Jersey State Government information security management framework as well as the responsibilities and expectations associated with these roles is as follows.

OR-02.1: INFORMATION SECURITY GOVERNANCE COMMITTEE (ISGC)
The ISGC shall be established and co-chaired by the Director of NJOHSP and the Chief Technology Officer. Membership will include the State CISO, State Chief Data Officer, Director of the NJCCIC, as well as representatives from the Governor’s Office, the Office of the Attorney General, the Civil Service Commission, the Department of the Treasury’s Office of Management and Budget, and other State agencies, as appropriate. The ISGC shall report to the Cabinet and be responsible for:

(a) Assisting the State CISO in overseeing and executing New Jersey’s information security management program;

(b) Reviewing the Statewide Information Security Policies and Standards—and subsequent amendments—to ensure their alignment with the Executive Branch of State Government business goals and objectives, risk tolerances, and statutory, regulatory, and contractual requirements;
(c) Providing direction and counsel regarding the assessment and management of information security risks and cyber threats to the State of New Jersey;

(d) Reviewing reports on major information security incidents and cases of non-compliance;

(e) Overseeing the response to information security incidents;

(f) Reviewing security metrics and trends regarding the overall performance of the information security program; and

(g) Staying abreast of cybersecurity threats to the Executive Branch of State Government through briefings and reports.

OR-02.2: DIRECTOR, NEW JERSEY OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

The Director of NJOHSP shall administer, coordinate, lead, and supervise New Jersey's counter-terrorism and preparedness efforts. The goal of the Office of Homeland Security and Preparedness is to coordinate emergency response efforts across all levels of government, law enforcement, emergency management, non-profit organizations, other jurisdictions, and the private sector, to protect the people of New Jersey. In addition, the Director shall be responsible for the strategic development, execution, and management of an effective and efficient information security program to manage cyber risks and ensure the confidentiality, integrity, and availability of the Executive Branch’s information assets. Additionally, the Director of NJOHSP shall:

(a) Oversee the response to information security incidents;

(b) Stay abreast of cybersecurity threats to the Executive Branch of State Government information and information systems; and

(c) Advise the ISGC through regular briefings and reports.

OR-02.3: STATE CHIEF TECHNOLOGY OFFICER (CTO)

The CTO leads NJOIT, which is responsible for providing and maintaining the information technology infrastructure of the Executive Branch of State Government, including all ancillary departments and agencies. The CTO provides vision and leadership for NJOIT and is responsible for coordinating and conducting all Executive Branch technology operations. The CTO directs the planning, implementation, and governance of enterprise Information Technology systems in support of the Executive Branch of State Government’s business objectives and operations, to improve cost-effectiveness, service quality, and mission development.

At the CTO’s direction, NJOIT fulfills the following responsibilities in support of the State’s Information Security Program:
(a) Design, acquisition, and implementation of enterprise IT systems in compliance with the Statewide Information Security Manual’s Policies and Standards set by the State CISO;

(b) Operation and support of IT systems in compliance with approved security procedures, including, but not limited to:
   
   (1) IT asset management;
   (2) Malware protection;
   (3) Patch management;
   (4) Web proxying and Content filtering;
   (5) Secure file exchange; and
   (6) Data encryption;

(c) Management of third parties providing managed information services to NJOIT and other State entities;

(d) Identity and access management;

(e) Disaster recovery planning and operations;

(f) Providing recommendations on policy and control enhancements to NJOHSP’s Division of Cybersecurity;

(g) Monitoring NJOIT’s IT environment to identify, contain, or eliminate unauthorized activity;

(h) Assisting in implementing the Information Security Incident Response Plan;

(i) Providing subject-matter expertise for technical issues regarding information security; and

(j) Executing the day-to-day security management of enterprise information, systems, and solutions through the application of controls as defined within the Statewide Information Security Manual’s Policies and Standards.

Guideline: Consistent with Executive Order 225, the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual, the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term “agency” includes NJOIT and all ancillary departments and agencies.
OR-02.4: STATE CHIEF INFORMATION SECURITY OFFICER (CISO)

The State CISO reports to the Director of NJOHSP and serves as head of NJOHSP’s Division of Cybersecurity. The State CISO shall establish and manage an information security program to ensure the confidentiality, integrity, and availability of the State of New Jersey Executive Branch’s information resources, systems, and services while promoting and protecting privacy and safety. The State CISO has overall responsibility for the development, implementation, and performance of the information security program by:

(a) Setting strategic information security planning across the Executive Branch of State Government;

(b) Publishing the Statewide Information Security Manual’s Policies and Standards;

(c) Developing, managing, and executing the statewide Information Security Incident Response Plan;

(d) Identifying security requirements to limit the risks associated with identified Executive Branch business objectives as defined by the Governor and the Heads of State agencies;

(e) Developing, maintaining, and interpreting the Statewide Information Security Manual’s Policies and Standards;

(f) Providing information security subject matter expertise to State agencies;

(g) Drafting and implementing an information security awareness and training program to be used by all State agencies;

(h) Providing security metrics to track the performance of the information security program; and

(i) Developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:

(1) Coordinating and conducting compliance and risk assessments of agencies and their information assets;

(2) Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;

(3) Conducting penetration tests of agency networks, applications, databases, and systems; and

(4) Conducting information security risk assessments of third parties with access to State of New Jersey information assets.
OR-02.5: DIRECTOR OF THE NEW JERSEY CYBERSECURITY COMMUNICATIONS AND INTEGRATION CELL (NJCCIC)

The NJCCIC, established within NJOHS’s Division of Cybersecurity, shall be the State’s Cybersecurity Information Sharing and Analysis Organization. The Director of the NJCCIC shall be responsible for:

(a) Developing and managing a cybersecurity information sharing and analysis organization to liaise with the National Cybersecurity and Communications Integration Center within the US Department of Homeland Security, other federal agencies, and other public and private sector entities on issues relating to cybersecurity;

(b) Coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors;

(c) Coordinating information sharing related to cybersecurity risks, warnings, and incidents, and providing support on cybersecurity incident response and cybercrime investigations;

(d) Providing information and recommending best practices on cybersecurity and resilience measures to public and private entities, including on information security and data protection;

(e) Developing and implementing a cybersecurity threat information exchange with appropriate sources, including public utilities and private industry;

(f) Implementing and monitoring a centralized Security Information and Event Management (SIEM) system and, where appropriate, identifying, containing, or eliminating unauthorized activity and other cyber threats;

(g) Developing and managing an incident reporting system;

(h) Developing and providing information security incident response assistance and subject-matter expertise, as required;

(i) Providing cyber threat intelligence reports, analysis reports, briefings, alerts, and trainings to private and public organizations; and

(j) Developing working relationships with external organizations, including law enforcement, the private sector, academia, Information Sharing and Analysis Organizations, Information Sharing and Analysis Centers, and regulatory authorities.

OR-02.6: NEW JERSEY CHIEF DATA OFFICER (CDO)

The State CDO reports to the State CTO and serves as the central point of guidance, leadership, vision and coordination of statewide data standards across the Executive Branch. At the CTO’s direction, the CDO coordinates the planning, implementation, governance and management of enterprise information and data initiatives. The State CDO fulfills the following responsibilities in support of the State’s Information Security Program:
(a) Establishing statewide procedures, standards, and best practices regarding the definition and identification of critical business data and datasets;
(b) Developing cross agency protocols for data sharing and integration;
(c) Monitoring and ensuring compliance with the statewide data procedures, standards, and policies;
(d) Providing subject-matter expertise for data issues and policy regarding information security; and
(e) Assisting the State CISO and providing support to enable and implement the Information Security Management Program.

OR-02.7: HEADS OF STATE AGENCIES (INCLUDES SECRETARIES, DIRECTORS, COMMISSIONERS, CHAIRPERSONS, OR EQUIVALENT HEAD OF A STATE ENTITY WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT)

Heads of State Agencies (includes Secretaries, Directors, Commissioners, Chairpersons, or equivalent head of a state entity within the Executive Branch of State Government) are responsible for their respective agency’s operations. Likewise, they are responsible for the overall protection and use of information assets owned, managed, or licensed by the agency. To these ends, they are charged with:

(a) Driving commitment and support for the information security program;
(b) Accepting risk on behalf of the agency;
(c) Assigning appropriate IT management responsibilities within their respective agency to a designee who has the responsibility for the implementation and management of information technology systems in support of agency goals and objectives, and in accordance with the Executive Branch of State Government’s Statewide Information Security Policies and Standards;
(d) Assigning appropriate responsibilities within their agency to a designee who has the authority and responsibility for ensuring the implementation of, and the adherence to, the Information Security Program; and
(e) Promoting adherence to information security policies and cyber awareness programs.

OR-02.8: AGENCY CHIEF INFORMATION OFFICER (CIO)

The Agency CIO shall be responsible for the direction, planning, and implementation of information technology systems in support of agency business goals and objectives. In accordance with the New Jersey Office of Information Technology standards, directives and enterprise information strategy, the Agency CIO directs the planning and implementation of the agency information technology systems.
The Agency CIO fulfills the following responsibilities in support of the State’s Information Security Program:

(a) Design, acquisition, implementation, and operation of IT systems in compliance with approved policies and standards;

(b) Operation/Support of IT systems in compliance with approved security procedures, including, but not limited to:
   (1) IT asset management;
   (2) Malware protection;
   (3) Patch management; and
   (4) Data encryption;

(c) Management of third parties providing managed information services to the agency;

(d) Identity and access management;

(e) Disaster recovery planning and operations in coordination with NJOIT;

(f) Providing recommendations regarding policy and control enhancements to the Division of Cybersecurity;

(g) Monitoring the agency IT environment and, where appropriate, identifying, containing, and eliminating unauthorized activity;

(h) Assisting in the implementation of the Information Security Incident Response Plan;

(i) Executing the day-to-day security management of information, systems, and solutions through the application of controls as defined within the Statewide Information Security Manual’s Policies and Standards; and

(j) Providing subject matter expertise for technical issues regarding information security.

Guideline: Consistent with Executive Order 225, the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term “agency” includes NJOIT and all ancillary departments and agencies.

**OR-02.9: AGENCY CHIEF INFORMATION SECURITY OFFICER (CISO)**

The Agency CISO shall be responsible for protecting and maintaining the confidentiality, integrity, and availability of information assets under his/her purview. The Agency CISO fulfills the following responsibilities in support of the Statewide Information Security Policies and Standards:
(a) Identifying security requirements to effectively limit cyber risks associated with the agency’s business goals and objectives;
(b) Implementing and promoting information security awareness within their respective agency;
(c) Ensuring compliance with the Statewide Information Security Manual’s Policies and Standards within their respective State agency, including, but not limited to:

1. Coordination of risk assessments and compliance audits with NJOHSP’s Division of Cybersecurity;
2. Coordination of vulnerability assessments of agency networks, applications, databases, and systems; and
3. Coordination of risk assessments of third parties having access to agency information assets;
(d) Assisting in the implementation of the Information Security Incident Response Plan; and
(e) Reporting all information security incidents to the NJCCIC.

OR-03: FUNCTIONAL ROLES AND RESPONSIBILITIES
In addition to the management structure as documented above, the implementation and support for the State’s information security program requires agencies to identify and assign appropriate personnel to the following functional roles and responsibilities.

OR-03.1: INFORMATION SYSTEM OWNER
The information system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information systems owner may also be referred to as the asset owner. The information system owner has the following responsibilities related to system security:

(a) Assigns the security categorization and criticality of the information system;
(b) In coordination with the information owner, asset custodians, and stakeholders, develops and maintains security plans and contingency plans for all general support systems and major applications under their responsibility, including documenting the business associations and dependencies of the system (e.g., linked IT resources and flows of information);
(c) Ensures contracts pertaining to the information system include provisions for necessary security;
(d) Ensures that the information system is deployed and operated in accordance with the System Security Plan and all applicable statutory, regulatory, contractual and policy requirements;
(e) Ensures that access to sensitive information is limited to those with a “need to know” or “need to use”;

(f) Ensures the system’s personnel are properly designated, monitored, and trained;

(g) Ensures the system’s users receive the requisite security training;

(h) Updates the system security plan whenever significant changes or updates occur;

(i) Advises the information owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management);

(j) Participates in certification and accreditation process for the system, as well as, risk assessments and audits regarding the system’s safeguards; and

(k) Reports and responds to information security incidents in accordance with the Incident Response Policy.

Guidelines: The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life cycle phase of the information system. Some agencies may also refer to information system owners as program managers or business/asset/mission owners.

**OR-03.2: INFORMATION OWNER**

The information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to systems security:

(a) Assigns the security categorization, ensuring the protection standard, and establishing the rules for the appropriate use of the information;

(b) Ensures the collection and handling of information is compliant with all applicable laws, regulatory, and contractual requirements, and policies;

(c) Ensures the collection of personal information is limited to that which is needed for legitimate business purposes and in accordance with all statutory, regulatory, contractual, and policy requirements, and is retained only as long as necessary;

(d) Provides proper notice of the collection of personal information in accordance with all statutory, regulatory, contractual, and policy requirements;

(e) Assists in the identification and assessment of the common security controls where the information resides;

(f) Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information is generated, stored, processed, or transmitted;
(g) Defines precautions for controlling access to, and preserving the security and integrity of, information assets that have been categorized as requiring such precautions;

(h) Authorizes access to the information in accordance with the security categorization of the information, and the legitimate business need for access to the information; and

(i) Participates in certification and accreditation process for the system, as well as, risk assessments and audits regarding the system’s safeguards.

Guidelines: The role of the information owner in the context of security differs from that of the data owner in the context of the data governance model.

**OR-03.3: ASSET CUSTODIAN**

Under the direction of the information system owner and the information owner, asset custodians are responsible for the technical implementation and management of information assets. Asset custodians have responsibility for the day-to-day operational-level functions on behalf of the information system owner and the information owner. Typically, asset custodians will include systems administrators, network administrators, database administrators, or other designated information technology personnel.

Asset custodians are responsible for ensuring that the assets are properly secured, maintained, are used for the purposes intended, and that information regarding the equipment is properly documented. The asset custodian is responsible for receipt, transfer, accounting, safeguarding, and destruction of an information asset (e.g. information system) commensurate with the information’s security categorization. Asset custodians have the following responsibilities related to information security:

(a) Assists in the development of the System Security Plans and contingency plans for all information systems under their purview;

(b) Implements technical security controls in accordance with the System Security Plan and all applicable statutory, regulatory, contractual and policy requirements;

(c) Complies with any additional security requirements established by the Information System Owner, the Information Owner and/or the Agency CISO;

(d) Develops and maintains documentation regarding the design, implementation, operation, and security of the information system;

(e) Maintains and updates the inventory of the components (servers, network hardware, software, operating systems, patch levels, etc.) that comprise the information system;

(f) Advises the Information System Owner, the Information Owner and the Agency CISO of vulnerabilities that may present a threat to the confidentiality, integrity, availability, and privacy of the information system and/or the information;

(g) Monitors the security of the information system and reports and responds to security incidents in accordance with the Incident Response Policy;
(h) Notifies the Information System Owner, Information Owner, and the Agency CISO of any actual or attempted violations of security policies, practices, and procedures;

(i) Participates in certification and accreditation process for the system, as well as, risk assessments and audits regarding the system’s safeguards; and

(j) Abides by all information security policies and standards.

**OR-03.4: AGENCY HUMAN RESOURCES (HR) PERSONNEL**

Agency Human Resources personnel shall fulfill the following responsibilities in support information security program:

(a) Assists in the development, distribution, communications, and enforcement of the Statewide Information Security Manual’s Policies and Standards;

(b) Coordinates and administers the employee screening and background check process;

(c) Notifies the Agency CIO or his/her designee of new employees’ security access privileges according to their role and responsibilities;

(d) Notifies the Agency CIO or his/her designee of updates to employees’ security access privileges according to changes in employment status, including promotions, transfers, and terminations;

(e) Administers the new employee orientation program which includes the requirement to complete the Information Security Awareness and Training within thirty (30) days of hire;

(f) In coordination with the Agency CISO assists with the administration and tracking of compliance with the Security Awareness and Training requirements;

(g) Assists in the investigation and handling of information security policy violations, as appropriate; and

(h) Reports information security incidents in accordance with the Incident Response Policy, and the respective agency incident response plan.

**OR-03.5: OFFICE OF THE ATTORNEY GENERAL PERSONNEL**

The Office of the Attorney General personnel shall fulfill the following responsibilities in support of the information security program:

(a) Protects the State’s intellectual property rights;

(b) Provides advice and counsel regarding policies and standards, legislation, regulations and contractual terms;

(c) Provides advice, counsel, and investigative support regarding information security incidents;

(d) Acts as the primary point of contact for external legal services related to information security incidents;
(e) Assists in the development and evolution of the Executive Branch of New Jersey State Government’s Statewide Information Security Manual to ensure currency with legislative and regulatory changes and obligations;

(f) Reviews contracts and agreements to ensure that information security-related issues are addressed;

(g) Assists with the development and execution of privacy and security agreements for services provided by third-party vendors; and

(h) Assists with the development and execution of information sharing agreements.

**OR-03.6: USER**

All Executive Branch agency full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities, collectively referred to as users, are individuals authorized to access, and have a need to use, State information assets as part of their assigned duties or in fulfillment of assigned roles or functions. Users are considered both custodians of the information assets and information they are provided for use in the performance of their duties and are required to uphold all applicable information security policies and standards.

(a) Users are responsible for protecting information assets against their accidental or unauthorized disclosure, modification, and destruction, and for assuring the confidentiality, integrity, availability, and privacy of information and information assets;

(b) Individuals acting in a supervisory or management capacity are responsible for information security within their respective supervisory area. This responsibility includes supporting and ensuring compliance with the Statewide Information Security Manual’s policies and standards; and

(c) All users are responsible for understanding and complying with requirements of the Statewide Information Security Manual’s policies and standards.

**OR-04: SEPARATION OF DUTIES**

Agencies shall implement a separation of duties for all roles and operations that can impact the security of their information assets including, but not limited to, the following:

(a) Individuals fulfilling governance, compliance, and auditing roles should be independent from the functions they audit;

(b) The separation of security administration through which individuals and groups are provided access to information assets and those who act in other capacities, including, but not limited to, systems administration, application development, database management, etc., should be implemented to the fullest extent practical to meet business and security objectives;
(c) Application development personnel should not have access to production data or systems-level technology;

(d) Systems administrators should not have access to application code that would allow for them to make changes to the code;

(e) Database administrator access should be sufficiently restricted such that they can perform administrative functions without the option to retrieve sensitive information;

(f) Administrative access to firewalls, routers, switches, and other networking equipment and systems should be limited to authorized networking personnel; and

(g) Administrative access to information security systems and technologies should be limited to authorized personnel.

**OR-05: CONTACTS WITH EXTERNAL ORGANIZATIONS**

The NJOHSP Division of Cybersecurity shall develop and maintain relationships with external organizations to stay abreast of current and emerging security issues. Additionally, the Division of Cybersecurity shall maintain appropriate contacts with external organizations and entities to ensure that appropriate actions can be quickly taken, and advice obtained, in the event of a security incident. These contacts should include, but are not limited to, the following:

(a) Law enforcement authorities;

(b) Regulatory agencies;

(c) Incident response management service providers;

(d) Information security professional organizations;

(e) Information technology and telecommunications service providers; and

(f) Others, as necessary, to protect the Executive Branch of State Government information assets.

**OR-06: INDEPENDENT REVIEW OF INFORMATION SECURITY PROGRAM**

The State Chief Information Security Officer shall periodically engage external assessors and auditors to conduct independent reviews of the Executive Branch of State Government information security program. In addition, the State CISO, in coordination with State agencies, will engage independent external assessors to ensure accreditation and certification of its information security program as it relates to the State’s statutory, regulatory, and contractual obligations.

**OR-07: REPORTING OF INCIDENTS**

All personnel are required to immediately report any suspected information security incident. Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
- Agency HR Representative;
• Agency IT Service Desk;
• Agency Information Security Office;
• NJOIT Enterprise Service Desk – 1.800.622.4357; or
• NJ Cybersecurity Communications and Integration Cell – 1.609.963.6900 x 7865 or https://homelandsecurity.nj.gov/report.html

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to, and including, termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

REFERENCES:
The requirements established in the Organizational Security policy have been derived from the following:
• NIST SP 800-53 Program Management (PM), Personnel Security (PS); and
• NIST CSF Identify/Governance (ID.GV).
COMPLIANCE (CP)

PURPOSE
The purpose of the Compliance Policy is to ensure safeguards are in place and State of New Jersey Executive Branch Agencies comply with all applicable policy, statutory, regulatory and contractual compliance obligations.

KEY TERMS
None. See Glossary in Appendix B for complete listing of terms.

CP-01: POLICY
Agencies shall ensure appropriate safeguards are implemented to protect information systems and sensitive information in accordance with all applicable policy, statutory, regulatory, and contractual compliance requirements.

This policy is supported by the following standards and guidelines.

Guidelines: Individual agencies have various legal, regulatory, and contractual compliance requirements based on their business services and operations, and the information they collect, store, process, and transmit. Some common statutory and regulatory requirements include IRS Publication 1075, Safeguards for Protecting Federal Tax Returns and Return Information, Health Insurance Portability Act (HIPAA), Family Education Rights Privacy Act (FERPA), Payment Card Industry – Data Security Standards (PCI-DSS), and others. Additionally, certain contractual obligations including Memorandums of Understanding (MOU) with other agencies, organizations, business partners, etc., may require that agencies implement enhanced controls beyond those included in this manual to satisfy the specific requirements within the applicable statutes, regulations, and contracts.

CP-02: SECURITY CONTROLS OVERSIGHT
The Agency Chief Information Security Officer (CISO) and his/her designated representatives shall create and maintain a control framework that captures statutory, regulatory, contractual, and policy requirements relevant to the agency’s programs of work and information systems. The Agency CISO and his/her designated representatives are responsible for establishing and maintaining a process to:

(a) Meet the information security requirements in the policies and standards delineated by the NJOHS Division of Cybersecurity in this Manual;
(b) Develop and implement policies, standards, procedures and guidelines to address agency-specific information security requirements;
(c) Document and implement controls necessary to satisfy all applicable statutory, regulatory, and contractual requirements regarding information security;
(d) Monitor the effectiveness of the agency’s information security controls and establish continuous monitoring processes that include:

1. A configuration management process for systems;
2. A determination of the security impact of changes to systems, applications, and operations;
3. Ongoing security control assessments, based on an Agency-defined prioritization of systems; and
4. Reporting the Agency’s state of security to appropriate agency and State officials;

(e) Continuously improve both protection and detection processes;

(f) Review the control framework at least annually to ensure new legislation, regulations, or other requirements are accounted for;

(g) Perform periodic reviews of the control framework to ensure that the agency addresses nonconformities with established policies, standards, procedures, and compliance obligations; and

(h) Maintain documentation of the reviews to include:

1. Documenting the results of the reviews; and
2. Review and sign-off of results by authorized personnel.

Guidelines: A control framework includes those controls dictated by the policies and standards contained in this Manual, as well as those required by applicable statutes, regulations, and contracts, as well as any agency-specific information security policies. Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security controls that support an agency’s risk management decisions. The terms continuous and ongoing imply that agencies assess and analyze security controls and information security-related risks at a frequency sufficient to support the agency’s security controls oversight.

**CP-03: SECURITY ASSESSMENTS**

Agency CISOs shall ensure security assessments of agency information systems are conducted in accordance with the Risk Management and Vulnerability and Patch Management policies for all significant development and/or acquisitions, prior to information systems being placed into production. In addition, Agency CISOs are responsible for:

(a) Coordinating and conducting prioritized compliance and risk assessments of the Agency’s information security controls and their information assets;

(b) Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;

(c) Coordinating information security risk assessments of third parties with access to agency information assets.
Guidelines: See the guidelines in the Risk Management and Vulnerability Management policies for additional information.

**CP-04: SECURITY ASSESSMENTS | FUNCTIONAL REVIEW OF SECURITY CONTROLS**

Agency CISOs are required to conduct periodic reviews of their information systems for compliance with the policies and standards included in this Manual and to document the results of the reviews.

(a) Periodic reviews are to be conducted on a defined frequency, based on the sensitivity of the information, the criticality of the system, and an analysis of the risks to the security of the system; and

(b) At a minimum, all systems should be reviewed on an annual basis.

Guidelines: Agencies should prioritize security assessments and increase the frequency of the assessments of systems with high impact security categorizations, and those that are highly exposed to threat actors, such as public facing websites, and as such are more likely to be targeted.

Agencies should maintain documentation describing the functional properties of the security controls employed within information systems, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. The purpose is to ensure that documentation is available to facilitate the testing of the implementation and/or operational issues associated with deployed security controls.

**CP-05: SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS**

As feasible, agencies will utilize independent assessors for security assessment functions.

Guidelines: Independent assessors should be used, where possible, in order to conduct impartial assessments of agency information security controls. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the agency’s information systems under assessment or to the determination of security control effectiveness. Individual assessors may include agency information security personnel, the NJOHSP Division of Cybersecurity personnel or external entities contracted by the agency.

**CP-06: SECURITY ASSESSMENTS | OFFICE OF HOMELAND SECURITY AND PREPAREDNESS**

To ensure appropriate safeguards are implemented throughout the Executive Branch of the New Jersey State Government, the Office of Homeland Security and Preparedness, Division of Cybersecurity shall coordinate and conduct periodic security assessments of agency information systems and controls. Security assessments will be completed on both the Agency and system levels, on a prioritized basis. NJOHSP shall:
(a) Coordinate and conduct compliance and risk assessments of agencies and/or their information assets;
(b) Conduct and manage vulnerability assessments of agency networks, applications, databases, and systems;
(c) Conduct and coordinate penetration tests of agency networks, applications, databases, and systems; and
(d) Conduct information security risk assessments of third parties with access to State of New Jersey information assets.

Agencies are required to cooperate with NJOHSP security assessments.

Guidelines: As appropriate, NJOHSP will coordinate security assessments with agency CIOs and CISOs to minimize any business disruptions. Assessments should be prioritized for systems that contain High Impact information, those considered to be Mission Critical to an agency’s operations, and those that are public facing, and as such are more likely to be targeted.

**CP-07: THIRD PARTY AUDITS**

As required by statute, regulation, or contract, agency information security controls may be subject to periodic audits by third-parties. Prior to commencing audit activities:

(a) Agencies are required to develop a detailed audit plan with all stakeholders to ensure there is minimal disruption to agency business while also allowing for the efficacy of the audit process;

(b) Agencies shall notify, and coordinate all planned third-party information security audits with, the Office of Homeland Security and Preparedness Division of Cybersecurity, and the Office of Information Technology.

All applicable agencies and their personnel shall cooperate with third-party audits as required by statute, regulation, and contract.

Guidelines: The proposed information security-related activity plan should be reviewed and vetted by agency management.

**REFERENCES**

The requirements established in the Compliance Policy have been derived from the following:

- NIST SP 800-53 Program Management (PM), Security Assessment and Authorization (CA);
- NIST CSF Protect/Information Protection Policies and Procedures (ID.PR), Identify/Governance (ID.GV); and
PERSONNEL SECURITY (PS)

PURPOSE
The purpose of the Personnel Security Policy is to ensure that all Executive Branch of New Jersey State Government personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

KEY TERMS
Access - Ability to make use of any information system or resource.

User – The term “user” refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to State information assets.

PS-01: POLICY
Agencies shall implement workforce security procedures to ensure that individuals with authorized access to agency information assets have the requisite skills and training to carry out their job functions. All full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities, shall have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

Agencies shall establish workforce security procedures that meet, or exceed, the minimum information security controls as listed below.

This policy is supported by the following standards and guidelines.

PS-02: SECURITY REQUIREMENTS WITHIN POSITION DESCRIPTIONS
Agencies are required to ensure that position descriptions include appropriate language regarding each role’s security requirements.

(a) Agency management shall be responsible for working with their respective Agency Human Resources representatives and Information Security Officers to identify security concerns associated with position responsibilities; and

(b) Position descriptions should be reviewed and updated as needed.

Guidelines: Agencies should refer to NIST Special Publication (SP) 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework for further information regarding security roles and responsibilities.
**PS-03: WORKFORCE SCREENING**

To the extent permitted by law, employment screening checks shall be conducted and successfully passed for all personnel prior to beginning work or being granted access to State information assets.

(a) Background screening requirements, as permitted by relevant laws and regulations, shall be included in all contracts with consultants, contractors and third-party vendors that are to be provided with access to State information assets;

(b) The level of background verification checks shall be commensurate with the role, responsibilities, and level of access to be granted;

(c) Supplemental employment screening may be required for personnel who are in key positions with privileged access to State information assets; and

(d) Individuals with access to information governed by statutory, regulatory, or contractual requirements shall be required to successfully pass criminal background checks in order to fulfill the responsibilities of the position. It is the responsibility of each agency to identify and ensure compliance with the policies, laws, contracts, and regulatory requirements that are applicable to the information assets they own, lease, license, or manage.

Guidelines: Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations, and ethics, and should be proportional to the business requirements, the security categorization of the information assets to be accessed, and the perceived risks.

Some methods of screening procedures include, but are not limited to:

- Previous employment history verification;
- Education checks;
- Personal/professional reference checks; and
- Criminal history record check.

Information types for which access requires the successful completion of a criminal background check includes, but is not limited to:

**Federal Tax Information (FTI)** – Federal Tax information consists of federal tax returns and return information (and information derived from it) that is in the agency’s possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(b) agreement. FTI
includes any information created by the recipient that is derived from Federal return or return information received from the IRS or obtained through a secondary source.

**Criminal Justice Information (CJI)** - Criminal Justice Information is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to: biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- **Biometric Data** - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, it can include: fingerprints, palm prints, iris scans, and facial recognition data.

- **Identity History Data** - textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

- **Biographic Data** - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

- **Property Data** - information about vehicles and property associated with a crime when accompanied by any personally identifiable information (PII).

- **Case/Incident History** - information about the history of criminal incidents.

Agencies should review the information they generate, process, store, or transmit to determine applicable laws governing access and background check requirements.

**PS-04: RULES OF BEHAVIOR**

Agencies are required to develop procedures to ensure personnel are aware of and understand usage policies applicable to State information and information systems as well as any agency-specific usage policies, ensuring:

(a) Information systems may only be used after explicit approval is given by agency management;

(b) User authentication must be enabled, where technically feasible; and

(c) Acceptable uses of State information assets must be given.

Guidelines: The Rules of Behavior - Acceptable Use of State Information Assets Policy covers the rules of behavior that are applicable to all users of State information assets.

**PS-05: TRANSFERS AND PROMOTIONS**

Agencies shall ensure that a review of security access and job responsibilities are performed by the releasing and receiving managers when an employee is promoted, transferred to another Department, Agency, or organization unit, or takes on a different role, to ensure appropriate access levels to information assets.
If an employee is given added responsibility at a key position through transfer or promotion, an additional background check and screening should be considered, if permitted and/or required by applicable laws and regulations.

**PS-06: PERSONNEL TERMINATION**

Agencies are required to ensure that upon termination of an individual’s employment:

(a) System access accounts are disabled;
(b) Exit interviews are conducted, if possible;
(c) All State-related property is recovered; and
(d) All State-owned information the terminated employee was responsible for is identified and accounted for;

If a user resigns or is terminated, the following should be accomplished at the time the user’s employment status is terminated:

(e) The user's privileges and access must be revoked;
(f) The user’s passwords must be changed or the accounts disabled to preclude access;
(g) All shared passwords known by the user on all applicable systems must be changed;
(h) All privileged account passwords known by the user must be changed;
(i) Incoming mail for the user should be re-directed, as prescribed by the user’s supervisor;
(j) After thirty (30) days, incoming mail should be disabled for the account, unless continuation is deemed necessary for business continuity;
(k) All files owned by the user should be identified and either archived, or ownership changed to a valid user;
(l) All automated scripts/ batch jobs previously requested or previously submitted should be reviewed; and
(m) All State property should be collected, including but not limited to:

1. Keys, lock combinations, and identification badges;
2. State-owned equipment, laptop computers, smartphones, tools and accessories;
3. Sensitive information and documentation; and
4. Program documentation.

**PS-07: REPORTING OF INCIDENTS**

Agencies shall develop procedures to ensure all personnel are aware of their duty to protect State information assets and their responsibility to immediately report any suspected information security incident. Suspected information security incidents may be reported via the following channels:
• Immediate supervisor;
• Agency HR Representative;
• Agency IT Service Desk;
• Agency Information Security Office;
• NJOIT Enterprise Service Desk – 1.800.622.4357; or
• NJOIT Enterprise Service Desk – 1.800.622.4357; or
• NJ Cybersecurity Communications and Integration Cell – 1.609.963.6900 x 7865

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to and including termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

REFERENCES
The requirements established in the Personnel Security Policy have been derived from the following:

• NIST SP 800-53 Personnel Security (PS), Planning (PL); Access Control (AC); Security Assessment and Authorization (CA);
• NIST CSF Protect/Information Protection Processes and Procedures (PR.IP);
• FBI Criminal Justice Information Security Policy; and
• IRS Publication 1075 - Safeguards for Protecting Federal Tax Returns and Return Information.
SECURITY AWARENESS AND TRAINING (AW)

PURPOSE
The purpose of the Security Awareness and Training Policy is to ensure users are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory and policy requirements that are intended to protect State information systems and information from a loss of confidentiality, integrity, availability, or privacy.

KEY TERMS
Computer-Based Training (CBT) – is any course of instruction for which the primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through an agency or the State intranet, or over the Internet as Web-based training.

AW-01: POLICY
Agencies shall ensure that all users are made aware of the security risks associated with their roles and that users understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of State information systems and information.

This policy is supported by the following standards and guidelines.

AW-02: INFORMATION SECURITY AWARENESS PROGRAM
The State Chief Information Security Officer (CISO) is responsible for developing and implementing an enterprise information security awareness program that is to be administered to all full and part-time employees, interns, volunteers, contractors, and those employed by contracted entities, by their respective agency CISOs.

(a) The information security awareness and training program shall be developed to make State personnel aware of the importance of information security, as well as to provide them with an understanding of State information security policies, laws, and regulations that govern their use of State information systems and information.

(b) The NJCCIC licenses an online computer-based training (CBT) information security and awareness program that all Executive Branch Agencies are to use to provide agency personnel with a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

Guidelines: Agency CISOs should contact the NJCCIC at cybertraining@cyber.nj.gov to request access to the NJCCIC-licensed CBT program. Agency CISOs may implement additional information security awareness requirements within their respective agency.
AW-03: INFORMATION SECURITY TRAINING

(a) Agency CISOs in coordination with agency HR personnel shall ensure that all new personnel complete security awareness training within thirty (30) business days of their start of employment as part of the required new hire training curriculum;

(b) Agency CISOs shall ensure that all users who have authorized access to State information systems complete security awareness training at least annually, to ensure that they are aware of their responsibilities with regard to information security; and

(c) Failure to complete the mandatory security awareness training may result in suspension of access to information assets.

Guidelines: Training should focus on developing and improving on core information security capabilities that are needed to protect organizational operations, assets, and individuals.

Initial orientation and ongoing security training should include the following topics:

- Information security basics;
- Information security policies;
- Rules of Behavior and Acceptable Use policies;
- Security categorization and handling;
- Information security threats related to the use of email - malware and phishing;
- Offsite security/security at home;
- Wireless security;
- Visitor security procedures;
- Incident response responsibilities; and
- Business continuity roles and procedures.

AW-04: ROLE-BASED SECURITY TRAINING

(a) As applicable, agency CISOs shall develop and provide users with information security training specific to their agency’s programs of work, applicable laws and policies, and information and systems.

(b) Agency CISOs shall ensure that specialized role-based security training is provided to individuals with significant information security related responsibilities. Agency CISOs shall ensure personnel assigned to these positions are appropriately trained.

Guidelines: Specialized role-based information security training may include such topics as secure coding for application developers, vendor or security product specific training for asset custodians, etc.
AW-05: INFORMATION SECURITY TRAINING RECORDS
Agencies shall implement processes that require agency personnel to acknowledge in writing or electronically, at least annually, that they have completed the required CBT training, and have read and understand the State’s information security policies.

Guidelines: Any distributed security bulletins or awareness training information should be archived as evidence of training. If possible, the individuals who received training or distribution list recipients should be documented. A record of the acknowledgment of cybersecurity training shall be maintained by the agency’s Human Resources department as evidence of training.

AW-06: SECURITY ADVISORIES AND ALERTS
The New Jersey Cybersecurity Communications and Integration Cell shall provide agencies with current and relevant security-related advisories and alerts on a periodic basis. Such alerts and advisories may be distributed via email, phone, text message, Internet or Intranet postings, or other communications medium, as appropriate. Each Agency CISO/ISO is responsible for ensuring these alerts and advisories are communicated to the appropriate personnel under their purview.

AW-07: INFORMATION SECURITY RESOURCES
The Division of Cybersecurity within the Office of Homeland Security and Preparedness shall create, post, maintain, and make available to all agencies any information security policy documentation, training materials, security guidelines, advisories, alerts, etc.

REFERENCES
The requirements established in the Security Awareness and Training Policy have been derived from following:

- NIST SP 800-53 Secure Awareness Training (AT), Program Management (PM); and
- NIST CSF Protect/Awareness and Training (PR-AT).
RULES OF BEHAVIOR - ACCEPTABLE USE OF STATE INFORMATION ASSETS (RB)

PURPOSE
The purpose of this policy is to establish required behaviors and provide direction to Executive Branch of New Jersey State Government personnel regarding their roles and responsibilities with respect to the acceptable use and security of State information assets.

KEY TERMS
Agency – The term “agency” is used to refer to any Department, Agency, Commission, Board, Body, or other instrumentality of the Executive Branch of New Jersey State Government.

User – The term “user” refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to State information assets.

Information Asset – An information asset is any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

RB-01: POLICY
The use of State information assets is permitted for authorized State government business purposes to support the goals and objectives of the Executive Branch of New Jersey State Government departments and agencies. Accordingly, State information assets are to be used in a manner that is consistent with applicable laws and regulations, in accordance with all New Jersey State Government policies, and as part of the individual’s assigned duties and responsibilities.

This policy is supported by the following standards and guidelines.

RB-02: AGENCY RESPONSIBILITY
(a) Agency management shall ensure users are provided with security awareness training in accordance with the Security Awareness and Training Policy. Users are to be made aware of the security risks associated with their roles, and understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of State information assets.

(b) Agency CISOs in conjunction with agency management shall develop rules of behavior and acceptable use requirements that, at a minimum, incorporate the rules and requirements below; and
(c) Agency managers shall be responsible for ensuring that users acknowledge in writing, or electronically, their understanding of, and agreement to abide by, the terms set forth in the Rules of Behavior and Acceptable Use of State Information Assets Policy.

Guidelines: Agency developed Acceptable Use and Rules of Behavior polices may contain more restrictive terms.

RB-03: USER RESPONSIBILITIES
The rules of behavior and requirements contained in this policy apply to all users of State information assets, regardless of the agency, role, or location:

(a) Users are responsible for the security and use of their user account and all State information assets, for which they are assigned;

(b) Unauthorized access to State information and/or systems is prohibited; and

(c) Users shall immediately report lost or stolen State information assets, suspected policy violations, suspected information security incidents, and suspicious activity, in accordance with their agency’s reporting procedures.

Guidelines: As noted in detail in the Incident Response Policy users may also use the following channels to report suspected policy violations, suspected information security incidents, and suspicious activity:

- Immediate supervisor;
- Agency HR Representative;
- Agency IT Service Desk;
- Agency Information Security Office;
- NJOIT Enterprise Service Desk – 1.800.622.4357; or
- NJ Cybersecurity Communications and Integration Cell – 1.609.963.6900 x 7865 or https://homelandsecurity.nj.gov/report.html

RB-04: ACCEPTABLE USE
Users shall:

(a) Protect and secure State of New Jersey information assets;

(b) Access sensitive information assets only to conduct official agency business and only as permitted by applicable laws, regulations, and policies;

(c) Users who store, transmit, or process State data using commercial cloud services must use services provided by or sanctioned by their respective agencies rather than personally obtained cloud services;

(d) Log off or lock systems when leaving them unattended;
(e) Complete security awareness training upon hire and on an annual basis thereafter;
(f) Permit only authorized users to use agency-provided information assets;
(g) Secure sensitive information (on paper and in electronic formats) when left unattended;
(h) Keep sensitive information out of sight when visitors or other individuals without authorization to view the sensitive information are present;
(i) Sanitize or destroy electronic media and papers that contain sensitive information when no longer needed, in accordance with records management and media sanitization policies;
(j) Only use personally identifiable information for the purposes for which it was collected.

RB-05: PROHIBITED USE

Users shall NOT:

(a) Perform any act that is illegal or otherwise in violation of any applicable Federal or State laws, or State policies;
(b) Circumvent security safeguards or reconfigure State information assets except as authorized;
(c) Access, transmit, store, or create any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate content including, but not limited to: websites that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone’s age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;
(d) Create, send, or forward any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate communications. Among those communications considered inappropriate are any communications or materials that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone’s age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;
(e) Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter;
(f) Send an email under another individual’s name or email address, except when authorized to do so by the owner of the email account for a work-related purpose;
(g) Use another user’s account, identity, or password;
(h) Download and install unapproved software applications on State owned, managed, or leased information assets;
(i) Establish new Internet web and/or social media pages or content dealing with State business, or make modifications to existing pages or content dealing with State business without authorization;

(j) Transmit, store, process, or share sensitive State information using personal or other unauthorized Internet services including but not limited to: personal email accounts, social media accounts, chat services, file storage, file synchronization, file sharing, and other unauthorized services;

(k) Exceed authorized access to sensitive information;

(l) Share sensitive information, except as authorized;

(m) Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization and appropriate safeguards (e.g. access controls, encryption), as stipulated by policy;

(n) Acquire, use, reproduce, transmit, or distribute any information, software or other electronic materials (e.g. movies, music) that are subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, transfer or export-controlled software or data;

(o) Use State information assets to conduct or promote an employee’s outside employment or business interests, including but not limited to consulting for pay, buying, selling, trading, or any secondary employment purpose;

(p) Use State information assets to conduct political activity such as lobbying elected officials and participating in partisan political activities; and

(q) Add or install personal IT resources (e.g. wireless access points, software, mobile devices, etc.) to existing State information systems without the appropriate management authorization.

RB-06: NO EXPECTATION OF PRIVACY
Information assets created, purchased, leased, or licensed by the State of New Jersey including but not limited to: software (e.g. application software, application source code, systems software), physical equipment (e.g. computers, portable devices, tablets, smartphones), communications equipment (e.g. routers, switches, firewalls), electronic media (e.g. disks, tapes), services (e.g. Internet, communications, cloud), and information (e.g. databases and data files, system documentation, network diagrams) are the property of the State of New Jersey. As such, the State has the absolute right to monitor the use of such property. Accordingly, users of State information assets shall not assume their actions or use of State information assets are private or protected.

RB-07: SECURITY MONITORING
In order to protect State information assets against security threats and to ensure compliance with the State and agency-specific policies, as well as applicable contractual, regulatory, and statutory requirements, State agencies have the right to implement security monitoring
technologies and systems, including but not limited to: anti-virus/anti-malware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention, and web and email content filtering systems. As permissible by law, the agencies’ security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log any traffic sent or received by users of State information assets, and any network traffic emanating from or sent to agency networks, systems, applications, databases or other information assets, as well as any traffic directed at the State’s information assets from external sources.

**RB-08: INCIDENTAL USE OF STATE OF NEW JERSEY INFORMATION ASSETS**

State of New Jersey information assets are provided for the purpose of conducting State business. Incidental use of State information assets for personal purposes is permitted when such use does not interfere with the user’s performance, does not expose the State to unnecessary risks, does not result in additional cost to State agencies, and does not violate any policies, applicable laws, regulatory, or contractual requirements.

Agencies and users’ managers may adopt more restrictive incidental use policies. Existing labor management agreements may preclude application of one or more of the incidental personal use guidelines listed below.

In addition:

(a) Users have no inherent right to use State information assets for personal use;

(b) Users must understand that any use of State information assets including email may not be secure, is not private, is not anonymous, and may be subject to monitoring. Users do not have a right to, nor shall they have an expectation of, privacy while using State information assets at any time, including accessing the Internet through State-provided connectivity. To the extent that users wish that their personal activities remain private, they shall avoid making personal use of State information assets;

(c) A user’s incidental personal use of State information assets does not extend to the user’s family members or others regardless of where the information asset is physically located;

(d) Storage of any user’s personal data, including but not limited to, personal email messages, photos, contacts, voice messages, files, or documents created as incidental use must be nominal and temporary;

(e) The State assumes no responsibility for the availability, confidentiality, integrity of any user’s personal data stored, processed, or transmitted using State information systems or assets;

(f) The State has no responsibility or obligation to provide access to or make copies of a user’s personal data upon the user’s separation from State Government employment, whether through voluntary or involuntary termination;
(g) Employees are prohibited from using State information assets to conduct or promote an employee’s outside employment or business, including but not limited to buying, selling, trading, or any secondary employment purpose; and

(h) Employees may not use State information assets to conduct political activity such as lobbying elected officials and participating in partisan political activities.

**RB-09: ADDITIONAL RULES FOR SECURITY AND PRIVILEGED ACCESS USERS**

Individuals, including but not limited to Information Technology personnel and Information Security personnel, with privileged access to State information assets shall:

(a) Only use privileged access credentials for duties that require escalated privileges;

(b) Use a standard user account for all other activities;

(c) Advise the Information System Owner and the Information Owners on matters concerning information security;

(d) Assist the Information System Owner and Information Owners in developing system security plans, risk assessments, and supporting documentation;

(e) Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need to know basis;

(f) Verify that users have received appropriate security training before allowing access to any system;

(g) Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs; and

(h) Document and investigate known or suspected security incidents or violations and report them in accordance with the Incident Response Policy.

Guidelines: Privileged access is also referred to as Administrator, Super User, or Root access and typically include roles such as Systems, Network, Domain and Database Administrators.

**RB-10: VIOLATIONS**

Violations of this policy may result in revocation of access to State information assets and/or disciplinary action including suspension or termination. In addition, violations may be subject to civil or criminal prosecution under Federal or State law.

**REFERENCES**

The requirements established in the Rules of Behavior – Acceptable Use of State Information Assets Policy have been derived from following:
• NIST SP 800-53 Personnel Security (PS), Security Assessment and Authorization (CA), Awareness and Training (AT); and
• NIST CSF Identify/Governance (ID.GV), Protect/Information Protection Policies and Procedures (ID.PR), Awareness and Training (AT), Detect/Security Continuous Monitoring (DE.CM).

RELATED POLICIES AND CONTROLS
• State of New Jersey Civil Service Commission Policies and Procedures
• New Jersey Conflicts of Interest Law
RISK MANAGEMENT (RM)

PURPOSE
The purpose of the Risk Management Policy is to establish requirements for the identification, assessment, and treatment of information security risks to agency operations, information systems, and information.

KEY TERMS
General Support System - a general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- Local area network (including workstations, printers, and other assets that support an agency office or facility);
- Backbone network (e.g. agency-wide and/or statewide (GSN));
- Agency data processing center including its operating system and utilities (e.g. server room); and/or
- Shared information processing service facility (e.g. data center).

Major Applications and Systems – a major application or system is described as any system or application that includes one or more of the following characteristics:

- Includes users in more than one agency;
- Costs more than $100,000 to develop and implement (cost includes hardware, software, and contract personnel);
- Any public facing web application; and/or
- Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

Minor Applications – consist of those systems and applications not considered major applications or general support systems. Often times minor applications are components of a major application or system.

Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, availability, and/or privacy of information or information systems and take into consideration the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, the State, and the Nation.

**Risk Assessment** - The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

**Risk Management** - The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State, resulting from the operation of an information system, and includes:

(i) the conduct of a risk assessment;
(ii) the implementation of a risk mitigation strategy; and
(iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

**Risk Mitigation** - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

**Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, the State, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**RM-01: POLICY**
Agencies shall implement continuous risk management processes that account for the identification, assessment, and treatment of risks that can adversely impact their operations, information and/or information systems.

This policy is supported by the following standards and guidelines.

**RM-02: RISK MANAGEMENT PROGRAM**
The State Chief Information Security Officer is required to develop and implement a statewide information security risk management strategy that includes:

(a) Formal risk assessments;
(b) Identification of critical assets, current safeguards, effectiveness of safeguards, threats, and vulnerabilities;
(c) A review of all processes involving creating, receiving, maintaining and transmitting of sensitive information; and
(d) Assigning responsibility to validate security controls.

**RM-03: RISK-BASED SECURITY CATEGORIZATION**

Agency CISOs shall:

(a) For all major applications and systems, and general support systems coordinate with the Information System Owner and Information Owner to complete and submit a System Security Plan (SSP) that categorizes the information and assets:

1. Prior to production implementation of new major systems and applications or general support systems;
2. When substantive changes have occurred in a major system or application, or general support systems;
3. After a breach of an asset’s information security controls; and
4. When substantive changes have occurred in the agency information technology or organizational environments;

(b) Complete a Privacy Impact Assessment (PIA) in accordance with the requirements contained in the Privacy Policy;

(c) In accordance with the State of New Jersey Technology Circular 195 – Contingency Planning Policy, Policy NO. 14-31-NJOIT, as well as the information security Contingency Planning Policy contained in this Manual, complete a Business Impact Assessment (BIA);

(d) Ensure the SSP, PIA, and BIA are reviewed and approved by the Agency CIO; and

(e) Submit the SSP, PIA, and BIA to the State Chief Information Security Officer or his/her designee and the State Chief Technology Officer or his/her designee for review.

**Guidelines:**

The security categorizations describe the potential adverse impacts on agency operations, agency assets, and individuals if agency information and information systems are compromised through a loss of confidentiality, integrity, or availability. The System Security Plan documents the controls and safeguards that are implemented to mitigate risks to the confidentiality, integrity, availability, and privacy of agency information and information systems. The SSP facilitates the development of inventories of information asset mappings to specific system components where information is processed, stored, or transmitted.

The PIA documents the privacy risks based on the personally identifiable information an information system generates, collects, shares, stores, uses, processes, or transmits. Both the SSP and the PIA are requirements for an information system to receive certification and authority to operate.
The BIA provides a method for determining the impact of any disruption to agency operations due to the loss of availability of an information system.

Copies of the SSP and PIA forms can be found on the NJCCIC Intranet site. Agencies can submit the SSP, PIA, BIA, and Risk Assessment reports to State Chief Information Security via email: RiskReview@cyber.nj.gov.

RM-04: RISK IDENTIFICATION
Agency CISOs shall implement processes to ensure risks are:

(a) Identified;

(b) Documented; and

(c) Assigned to the appropriate personnel for remediation action or acceptance of risk by the information system owner or information owner.

RM-05: RISK ASSESSMENTS
Risk assessments shall be conducted throughout the lifecycle of major systems and applications and general support systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met, and that risk will be mitigated and managed to an acceptable level. Risk assessments are to be conducted:

(a) Prior to production implementation of new major systems and applications, or general support systems;

(b) When substantive changes have occurred in a major system or application, or general support system;

(c) After a breach of a system’s information security controls;

(d) When substantive changes have occurred in the agency information technology or organizational environments; and

(e) At least annually, based on the criticality of the system and the sensitivity of the information.

Guidelines: Risk assessments are an ongoing process for all systems. The annual assessments of existing major systems and applications and general support systems, should be prioritized based on their criticality, the sensitivity of the information the systems process, store, and transmit, as well as statutory, regulatory, or contractual requirements regarding frequency of risk assessments.
RM-06: RISK ASSESSMENT COMPONENTS

Risk assessments shall include the following component activities:

(a) System characterization – identify and document:
   (1) Information assets that are within scope;
   (2) Security categorizations; and
   (3) Statutory, regulatory, contractual and policy requirements;

(b) Threat Identification – Identify and document potential threats and their sources Threats are commonly categorized as:
   (1) Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluxuation, etc.;
   (2) Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, spam, vandalism, etc.;
   (3) Natural – fires, floods, electrical storms, tornados, etc.;
   (4) Technological – server failure, software failure, ancillary equipment failure, etc.; and
   (5) Other – explosions, medical emergencies, misuse or resources, etc.

(c) Vulnerability Identification - Develop a list of technical and non-technical vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an agency’s computer usage to insufficient safeguards to protect facilities that house computer equipment, to any number of software, hardware, or other technical vulnerabilities;

(d) Control Analysis - Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented to minimize, or eliminate, the likelihood of a threat-source exploiting a vulnerability;

(e) Likelihood Determination - Determine the overall likelihood that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls;

(f) Impact Analysis - Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability;

(g) Control Recommendations - Identify controls that could reduce or eliminate the identified risks, as appropriate to the agency’s systems and/or operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, operational impact, and safety and reliability; and

(h) Report – Document the results of the risk assessment in an official report, spreadsheet, or briefing and submit to agency senior management and the State Chief Information Security Officer or his/her designee for review.
Guidelines: When completing a risk assessment report, Agency CISOs must apply a risk estimation methodology (either qualitative or quantitative) to measure risk levels, an estimation of the level of risk with appropriate values assigned, and an evaluation and prioritization of the risks in relation to incident scenarios and risk levels. Agency CISOs must also consider legal and regulatory risks when completing the risk assessment report.

**RM-07: RISK TREATMENT**

Agencies shall ensure that:

(a) Risks are mitigated to an acceptable level; and

(b) Remediation actions are prioritized based on risk criteria; and

(c) Timelines for remediation are established.

Agencies may choose to accept the risk. Risk acceptance processes must be followed with the appropriate level of approvals required commensurate with the level of risk.

Guidelines: Agencies are to prioritize risk remediation efforts based on the risk ranking, which includes the severity of the vulnerability, the likelihood that the vulnerability will be exploited, the impact that a loss of confidentiality, integrity, availability, or privacy would have, the statutory, regulatory, and contractual requirements, and other agency business related considerations.

**RM-08: RISK ASSESSMENT UPDATES**

Agencies are required to continually monitor systems under their purview and update risk assessments whenever there are significant changes to the system, a breach of the system’s security has occurred, the environment of operation has changed, or other conditions that may impact the security state of the system have emerged.

**REFERENCES**

The requirements established in the Risk Management Policy have been derived from the following:

- NIST SP 800-53 Program Management (PM), Risk Assessment (RA); and
- NIST CSF Identify/Governance (ID.GV), Identify/Risk Assessment (ID.RA).
PURPOSE
The purpose of the Privacy Policy is to establish appropriate processes and safeguards necessary to protect the personally identifiable information (PII) that agencies collect, store, and transmit.

KEY TERMS
Data - A subset of information in an electronic format that allows it to be stored, retrieved or transmitted.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Non-Sensitive Personally Identifiable Information (PII) - is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

Personally Identifiable Information (PII) - any information about an individual maintained by an agency, including:

(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Privacy – Freedom from unauthorized intrusion or disclosure of information about an individual.

Privacy Officer - Individual who is responsible for the oversight of the agency’s compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information.

Sensitive Personally Identifiable Information (SPII) – is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

PR-01: POLICY
Agencies shall implement appropriate processes and safeguards to protect the personally identifiable information (PII) that they collect, store, and transmit.

This policy is supported by the following control standards and guidelines.
PR-02: GOVERNANCE AND PRIVACY PROGRAM

Agencies shall:

(a) Appoint a senior agency official as a Privacy Officer, who is accountable for developing, implementing, and maintaining an agency privacy program to ensure compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by agency information systems;

(b) Monitor State and Federal privacy laws for changes that affect the agency’s privacy program;

(c) Allocate resources to implement and operate the organization-wide privacy program;

(d) Develop and implement privacy training and awareness aimed at ensuring users understand their privacy responsibilities;

(e) Ensure that the public has access to information about its privacy program;

(f) Ensure that its privacy practices are publicly available through agency websites and other communications mediums; and

(g) Update the privacy plan, policies, and procedures, at least annually.

Guidelines: By the very nature of the services the State and its ancillary agencies provide to the public, they collect vast amounts of personally identifiable information. The Agency’s privacy program and governance structure demonstrates its accountability for the commitment to individual privacy.

PR-03: PRIVACY IMPACT ASSESSMENT

Agencies shall implement a privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

(a) Agencies shall conduct Privacy Impact Assessments (PIA) for new information systems, systems under development, systems undergoing changes or upgrades, or other activities that pose a privacy risk;

(b) Agencies shall ensure a PIA is conducted prior to any new collection of PII, or upon significant changes in the architecture, information flow, or use of PII within existing systems;

(c) The Privacy Impact Assessment shall be documented and used by the agency to identify and implement appropriate controls necessary to protect PII in accordance with all applicable State and Federal laws, regulations, and internal agency policies; and

(d) Agencies shall submit the PIA to the State Chief Information Security Officer.
Guidelines: The Privacy Impact Assessment is intended to identify privacy risks that exist in new systems, systems under development, and systems undergoing change. The Privacy Impact Assessment Form can be found on the NJCCIC Intranet site

**PR-04: AUTHORITY TO COLLECT**

Agencies shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally, or in support of a specific program or agency information system need.

**PR-05: PRIVACY NOTICE**

Asset owners and asset custodians shall implement mechanisms that provide effective notice to the public and to individuals regarding:

(a) Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;

(b) Its authority and purpose for collecting PII;

(c) The choices, if any, individuals may have regarding how the agency uses PII and the consequences of exercising or not exercising those choices;

(d) The ability, if any, for individuals to access and have PII amended or corrected if necessary; and

(e) Updates for changes in the agency’s privacy practices, including changes in the use of personal information.

Guidelines: Additional privacy notice requirements are contained in The State of New Jersey Technology Circular, *On-Line Privacy Policy, 13-09-OIT*. The privacy notice enables individuals to understand how the agency uses PII generally and, where appropriate, to make an informed decision prior to providing PII to the agency.

**PR-06: CONSENT**

For collection, use, and disclosures of PII not already authorized by law, agencies shall, where feasible:

(a) Obtain consent from individuals to authorize the collection, use, storage, and sharing of PII prior to its collection;

(b) Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

(c) Obtain consent from individuals prior to any new uses or disclosure of previously collected PII; and

(d) Ensure that individuals are aware of and consent to all uses of PII not initially described in the public notice that was in effect at the time the agency collected the PII.
Guidelines: For systems and programs of work where the collection of PII is not already authorized by law, agencies may achieve awareness and consent, through appropriate public notice that contains enough details so that individuals can provide informed consent.

**PR-07: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION**

Agencies shall:

(a) Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

(b) Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice, and for which the individual has provided consent;

(c) As technically feasible, identify, redact, anonymize, or dispose of PII that is not necessary for the authorized purpose; and

(d) Conduct periodic reviews of the agency’s PII holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the authorized purpose.

Guidelines: The collection and storage of unnecessary PII elements introduces unnecessary risks and should be avoided where feasible.

**PR-08: DATA QUALITY**

Agencies shall implement and document processes to:

(a) Confirm to the greatest extent possible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

(b) Collect PII directly from the individual to the greatest extent practicable;

(c) Check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems; and

(d) Ensure the integrity of PII through existing security controls.

Guidelines: Agencies can take reasonable steps to confirm the accuracy of PII, such as validating input as PII is collected. This may include enforcing input restrictions to ensure SSN or telephone number fields only allow for numbers, or by validating addresses using automated address verification look-up application programming interfaces (APIs). The types of measures taken to protect data quality may be based on the nature and context of the PII, how it is to be used, and how it was obtained.

**PR-09: INTERNAL USE AND DISPLAY OF PERSONALLY IDENTIFIABLE INFORMATION**

Agencies shall:
(a) Use PII internally only as authorized by law, or for the authorized purpose(s) described in the privacy notice; and

(b) Mask Sensitive Personally Identifiable Information (SPII) that is displayed or printed. This includes, but is not limited to:

1. Financial account numbers;
2. Social Security Numbers (SSN); and
3. Credit or debit Primary Account Numbers (PANs) (no more than the first six (6) and last four (4) digits allowed to be displayed).

Guidelines: To reduce the exposure of sensitive PII agencies are to implement controls that mask sensitive PII and only provide access to the unmasked identifiers to those with a required business need.

In accordance with the Security in Software Development Policy, agencies are prohibited from using sensitive PII in test and development environments. Agencies are to use test, or dummy data, during the development and testing of information systems, information system components, and information system services.

**PR-10: PRINCIPLE OF LEAST PRIVILEGE**

Agencies shall employ the principle of least privilege in order to limit access to personally identifiable information to only those users who have a business need and require access to carry out their duties and responsibilities.

(a) Asset owners and custodians shall implement logical access controls in accordance with the Access Management and Identity and Authorization policies included in this Manual;

(b) Authorized individuals performing functions requiring privileged access must use designated privileged accounts only for administrative activities, and use standard user accounts for all other purposes;

(c) The principle of least privilege is also to be applied to programs and processes; and

(d) The principle of least privilege is extended to the display of SPII.

Guidelines: The concept of least privilege is to be applied for specific duties and information systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions.

**PR-11: INDIVIDUAL ACCESS**

In accordance with applicable State and Federal laws and regulations, and subject to any applicable exceptions or exemptions, agencies shall:
(a) Provide individuals the ability to have access to their PII maintained in its system(s) of records;

(b) Publish rules and regulations governing how individuals may request access to records maintained in a system of records; and

(c) Adhere to requirements, policies and guidance for the proper processing of PII requests.

PR-12: REDRESS
For collection, use, and disclosures of PII not already authorized by law, agencies shall:

(a) Provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and

(b) Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notify affected individuals.

Guidelines: Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations apply discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes.

PR-13: USER FEEDBACK MANAGEMENT
For collection, use, and disclosures of PII not already authorized by law, agencies shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about the agency’s privacy practices.

PR-14: INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION
Agencies shall:

(a) Establish, maintain, and regularly update an inventory that contains a listing of all programs and agency information systems identified as collecting, using, maintaining, or sharing PII; and

(b) Provide periodic reports of the agency’s use of PII to the State Chief Information Security Officer and the State Chief Technology Officer to support the establishment of information security requirements for all information systems containing PII.

Guidelines: Additional information regarding Sensitive Data Inventories can be found in the Media Protection Policy contained in this Manual.
PR-15: INFORMATION SHARING
Agencies shall:

(a) Share PII with third parties, only as authorized by law, or for the authorized purposes identified and described in the privacy notice, or in a manner compatible with those purposes;

(b) Where appropriate, enter into Information Sharing Agreements, Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, Service Level Agreements, Business Associate Agreements, or similar agreements, with third parties that specifically describe the PII covered, and specifically enumerate the purposes for which the PII may be used, and offers the same level of protection as documented in this policy;

(c) Monitor, audit, and train agency staff on the authorized sharing of PII with third parties; and

(d) Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new privacy notice is required.

PR-16: PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS
Agencies shall:

(a) Include privacy requirements in contracts to establish privacy roles and responsibilities for contractors and service providers;

(b) Obtain commitments from vendors and other third parties that have access to PII processed by the system, to notify the agency in the event of actual or suspected unauthorized access to, or disclosures of, PII; and

(c) Communicate privacy commitments and the associated system requirements to external users, as appropriate, to enable them to carry out their responsibilities.

Guidelines: Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing system development, information technology services, and other outsourced applications.

PR-17: PRIVACY INCIDENT RESPONSE
Agencies shall:

(a) Respond to information security incidents involving PII consistent with the Incident Response Policy contained in this Manual and the agency’s internal incident response plan;

(b) Provide timely notice to the State Chief Information Security Officer; and
(c) If the incident involves the breach of personal information as defined in the New Jersey Identity Theft Prevention Act, provide timely notification to the New Jersey State Police, and others, in accordance with all applicable laws and regulations.

Guidelines: According to the New Jersey Identity Theft Prevention Act, "Personal information means an individual's first name or first initial and last name linked with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or State identification card number; or
3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.”

Based on the PII that may have been accessed or disclosed without authorization, agencies may have additional reporting requirements.

**PR-18: PRIVACY AWARENESS AND TRAINING**

Agencies shall:

(a) Develop and implement privacy awareness and training aimed at ensuring users understand their privacy responsibilities;

(b) Administer basic privacy training annually, and targeted, role-based privacy training for agency users having responsibility for PII or for activities that involve PII; and

(c) Ensure that agency employees and contractors certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

**PR-19: DATA RETENTION AND DISPOSAL**

Agencies shall:

(a) Retain each collection of PII for an agency-defined time period to fulfill the purposes identified in the notice, or as required by State and Federal laws, regulations, and policies regarding records retention; and

(b) Dispose of, destroy, erase, and/or anonymize the PII, in accordance with the media sanitization requirements as documented in the Media Protection Policy contained in this Manual.

REFERENCES
The requirements established in the Privacy Policy have been derived from the following:

- NIST SP 800-53 Appendix J – Privacy Controls; and
- NIST CSF Identify/Governance (ID.GV).
PURPOSE
The purpose of this policy is to establish controls necessary to protect information assets from loss of confidentiality, integrity, and availability.

KEY TERMS
Information Asset – An information asset is any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

General Support System - a general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- Local area network (including workstations, printers, and other assets that support an agency office or facility);
- Backbone network (e.g., agency-wide and/or statewide (GSN));
- Agency data processing center including its operating system and utilities (e.g. server room); and/or
- Shared information processing service facility.

Major Applications and Systems – a major application or system is described as any system or application that includes one or more of the following characteristics:

- Includes users in more than one agency;
- Costs more than $100,000, to develop and implement (cost includes hardware, software, and contract personnel);
- Any public facing web application; and/or
- Any application that stores or processes sensitive information or is deemed critical to the operations of the agency

Minor Applications – consist of those systems and applications not considered major applications or general support systems. Often times minor applications are components of a major application or system.
**AM-01: POLICY**
Agencies shall implement administrative, technical, and physical controls necessary to safeguard information assets in all their forms from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate or accidental. The degree of protection for information assets will be based on the security categorization of the asset and the risks and consequences associated with having the security of the asset compromised.

This policy is supported by the following standards and guidelines.

**AM-02: INFORMATION ASSET IDENTIFICATION AND INVENTORY**
Agencies shall establish procedures to identify and maintain an accurate inventory of all State-owned, leased, licensed, or managed information assets. This inventory shall include all information necessary to recover from a disaster, including the description and value of the resource, the information owner and custodian, authorized users, and the resource’s security categorization.

Examples of information assets include but are not limited to:

(a) Information: databases and data files, system documentation, network diagrams, user manuals, training materials, operational procedures, disaster recovery plans, archived information;

(b) Software: application software, application source code, system software, development tools and utilities;

(c) Equipment: physical equipment (e.g., desktop and laptop computers, portable devices, tablets, smartphones), communication equipment (e.g., routers, switches, firewalls), magnetic and optical media (e.g., tapes and disks); and

(d) Services: locally hosted and cloud computing and communications services.

Agencies shall, at a minimum, review and physically verify all inventory components on a yearly basis. More stringent review timelines may be put in place per Agency needs.

Guidelines: Agencies should update the inventory as an integral part of component installations, removals, and information system updates. Without an inventory, some system components could be forgotten, and may be inadvertently excluded from applicable configuration standards. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the agency’s network.
AM-03: UPDATES DURING INSTALLATIONS, REMOVALS, UPDATES, AND MAINTENANCE

Agencies must update the inventory of information system components as an integral part of component installations, removals, and information system updates.

Guidelines: If any equipment needs to be taken for off-site maintenance to be performed, this should be documented using a State-Owned Property Removal Form and tracked in the inventory system.

AM-04: AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Where technically feasible, agencies shall implement IT Asset Management (ITAM) technologies that employ automated mechanisms to detect and isolate unauthorized hardware, software, and firmware components within a network or other information system.

Guidelines: Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

AM-05: NETWORK ACCESS CONTROL (NAC)

Where technically feasible, agencies shall deploy Network Access Control (NAC) technologies or other automated mechanisms to detect, isolate, and notify agency officials when unauthorized components/devices are added into agency networks or other information systems.

Guidelines: Agencies may deploy network level authentication via 802.1x or other technologies to limit and control which devices can be connected to the network. The network level authentication technologies such as 802.1x are to be tied into the inventory data to determine authorized versus unauthorized device or components. Client certificates may be used to validate and authenticate systems prior to connecting to the GSN.

AM-06: DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING

Where agencies use Dynamic Host Configuration Protocol (DHCP) to dynamically assign Internet Protocol addresses, and where technically feasible, DHCP events are to be logged to improve the asset inventory and aid in detecting unauthorized systems on the network.

AM-07: SOFTWARE LICENSING RESTRICTIONS

Agencies shall implement appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
Agencies are required to employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution, and to ensure use in accordance with contractual agreements and copyright laws.

Guidelines: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on agency needs.

**AM-08: ASSIGNING CUSTODIANSHIP OF ASSETS**

Agencies shall implement the following requirements for property accountability:

(a) All persons entrusted with State property are responsible for its proper use, care, custody, safekeeping, and disposition. Responsibility for items will be assigned in writing;

(b) Persons will not be assigned to a duty that will prevent them from exercising proper care and custody for the property for which they are responsible;

(c) When an individual assumes accountability for property that is remotely located, records must be maintained to show the location of the property and the persons charged with its care and safekeeping;

(d) State property will not be used for any private purpose except as authorized by agency management;

(e) No State property will be sold, given as a gift, loaned, exchanged, or otherwise disposed of unless specifically authorized by agency management; and

(f) Property documents shall identify the manufacturer’s make, model, and serial number.

Guidelines: Agencies should employ an automated mechanism to help maintain an up-to-date, complete, accurate, and readily available inventory of assets and system components.

**AM-09: ACCEPTABLE USE OF STATE INFORMATION ASSETS**

Prior to the assignment of information assets to personnel, agencies shall ensure that individuals are aware of their responsibility and accept their duty to protect State information and information assets. The requirements and terms of use of State information assets, are described in the Rules of Behavior – Acceptable Use of State Information Assets Policy.

**AM-10: RETURN OF ASSETS**

All individuals assigned custodianship of State information assets shall return all of the agency assets in their possession upon termination of their employment, contract or agreement.

The direct manager of a terminated user is responsible for inventorying and accounting for all agency assets, prior to the individual’s departure.
AM-11: REMOVAL OF ASSETS

Agencies shall implement processes to authorize, monitor, and control the removal, relocation or transfer of hardware, software, or data to offsite premises. Assets are prohibited from being removed from agency facilities without prior management authorization. Agencies shall complete a State-Owned Property Removal Form and track the removal of the assets in the inventory system.

AM-12: USE OF PERSONAL DEVICES

Within agency facilities, the use of personally owned technology assets shall be restricted.

(a) Personally owned technology assets are prohibited from:

(1) Connecting to any agency information system;

(2) Connecting to an agency’s internal network; or

(3) Being used in restricted areas.

(b) With management approval, personally owned technology assets are allowed to:

(1) Connect to the guest wireless network; and

(2) Remain in possession of the employee within the facility.

Guidelines: Employees are strongly encouraged to discuss the usage of personally owned technology assets with their immediate supervisor(s) for specific guidance. Personally owned technology assets include, but are not limited to:

- Personal smartphones and tablets;
- Storage devices;
- Digital photo frames; and
- Digital music players.

AM-13: USE OF THIRD-PARTY DEVICES

Assets belonging to and accessed by third parties (e.g. vendors, business partners, etc.) are prohibited from connecting to the GSN without prior authorization by agency management. The safe installation, maintenance and removal of third-party assets must be ensured through the following:

(a) All third-party assets must be assigned an NJOHSP asset custodian;

(b) Third-party assets must be documented in the asset inventory, to include third-party contact information;

(c) Asset custodians must document how and when the third-party owner is authorized to access the asset;
(d) The third-party must make provisions for the periodic verification of the asset’s functionality and the continued use on NJOHSP’s network; and

(e) Third-party assets cannot be removed without first purging all of NJOHSP’s sensitive data.

Guidelines: The third-party’s Statement of Work (SOW) should specify the necessary equipment, support and connectivity a third-party resource may need in an NJOHSP facility.

REFERENCES

The requirements established in the Security Categorization Policy have been derived from the following:

- NIST SP 800-53 Configuration Management (CM), Program Management (PM), Access Controls (AC); Risk Assessment (RA), Contingency Planning (CP), Security Assessments (CA), Systems and Services Acquisition (SA); and
- NIST CSF Identify/Asset Management (ID.AM).
PURPOSE
The purpose of the Security Categorization Policy is to establish security categorizations that are used to drive the implementation of controls necessary to protect information assets commensurate with the risks and impacts should there be a loss of confidentiality, integrity, and/or availability.

KEY TERMS
Authorization Boundary - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Availability - In the context of information security, refers to ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system.

Confidentiality - The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Data - A subset of information in an electronic format that allows it to be stored, retrieved or transmitted.

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Sensitivity - is the characteristic that defines either the value or importance of information. The degree of sensitivity is related to the negative consequences if the information were disclosed to unauthorized parties, destroyed, or lost. Information is classified in terms of its sensitivity, based on what it is and how access, communication and storage of it must be controlled.

Integrity - The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Nonpublic Information - Information that the employee obtains, or is provided access to, during
his/her employment with the State of New Jersey that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:

(a) Is designated by the State or the Agency for which the employee works as nonpublic information;

(b) Contains markings such as “Confidential”, “Internal”, “For Official Use” or similar language, or is considered sensitive information;

(c) Contains information that must be protected by State or Federal statute, State or Agency policy, or other regulation;

(d) Is provided to the State or the Agency for which the employee works by individuals or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or

(e) Contains information related to the internal State or Agency capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls.

**System** - a system is defined as a discrete set of information technologies including computer hardware, software, databases, etc., organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**SC-01: POLICY**

Information System Owners in conjunction with Information Owners, Agency CISOs, Privacy Officers, and other key stakeholders shall categorize assets and information according to their sensitivity and criticality. Protection mechanisms shall be implemented commensurate with the impact should there be a loss of confidentiality, integrity, and/or availability of the asset or information.

This policy is supported by the following standards and guidelines.

**SC-02: SECURITY CATEGORIZATION**

Agencies shall use the following impact levels when assigning security categorizations.

**Low Impact**: The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the State of New Jersey. i.e.

1. Causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
2. Results in minor damage to organizational assets;
3. Results in minor financial loss; or
4. Results in minor harm to individuals.
**Moderate Impact:** The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the State of New Jersey. i.e.

1. Causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in significant damage to agency assets;
3. Results in significant financial loss; or
4. Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

**High Impact:** The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the State of New Jersey. i.e.

1. Causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in major damage to organizational assets;
3. Results in major financial loss; or
4. Results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).

**SC-03: ASSIGNING SECURITY CATEGORIZATIONS**

Security categorizations shall be used to determine the security controls and protective measures that are to be applied to mitigate the risks of a loss of confidentiality, integrity and/or availability of assets and information.

(a) Asset and information must be categorized for each of the following security objectives:

   (1) Confidentiality;
   (2) Integrity; and
   (3) Availability

(b) Systems shall inherit the categorizations of the information which they generate, store, process, or transmit, and are to be protected accordingly;

(c) If more than one categorization could apply to a system or asset, the highest level (most restrictive) shall be applied; and

(d) Security controls must fulfill the defined protection requirements and provide an acceptable level of risk;

Guidelines: When assigning security categorizations to assets and information agencies should document the categorization results, including supporting rationale for the categorization. Agencies must ensure all assets within an authorization boundary to which a given asset is connected have required controls applied in accordance its security categorization. Security
categorization processes carried out by agencies facilitates the development of inventories of information assets and mappings to specific information system components where information is processed, stored, or transmitted. Security categorizations are key elements and should be included in service level agreements and other contract vehicles with service providers. Additional guidance regarding security categorizations can be found in Appendix A of this Manual.

SC-04: RISK CONSIDERATIONS
Agencies must account for the following risks when applying security categorizations:

(a) Health and Public Safety Risk: Loss of confidentiality, integrity or availability would jeopardize the health or safety of individuals;

(b) Operational Risk: Loss of confidentiality, integrity, or availability could prevent an agency, an agency function, or the State from accomplishing its core functions;

(c) Financial Risk: Loss of confidentiality, integrity, or availability would result in a loss of revenue, or criminal and civil penalties;

(d) Legal Risk: Some information is mandated by statute, regulation, and/or contract to be protected from a potential loss of confidentiality, integrity, or availability; and

(e) Reputation Risk: Loss of confidentiality, integrity, or availability would result in damage to the State’s or a State agency’s reputation.

SC-05: LABELING
Labeling is the practice of marking an information asset according to the information’s sensitivity so that others know how to handle the information. Agencies shall implement processes to ensure systems and documents are appropriately labeled. The following labels are to be applied to information assets:

(a) Public - The term public information applies to information intended for release to the public without restriction. Public information is disseminated to the public via authorized channels and is information expressly authorized for public disclosure or is obtained exclusively through the public domain.

(b) Confidential - The term confidential information applies broadly to non-public information intended for official use by employees, contractors, and other authorized third-parties when conducting State business. The term also applies to the most sensitive confidential information that is subject to more stringent protection measures and typically falls under statutory, regulatory, contractual, or other State policy requirements. Access to confidential information is generally restricted to individuals with a legitimate need.

Acceptable alternative labels for confidential information include:

• Internal
Agencies may develop agency-specific alternate labels that denote the information’s sensitivity, so long as the label provides others with information on how to handle the information.

Guidelines: An alternate labeling construct that is used to share information is the US-CERT Traffic Light Protocol (TLP).

Labels are intended to inform others on how to handle the information. They do not prescribe the controls that are to be implemented to protect the information asset from a loss of confidentiality, integrity, or availability.

Public information does not require a label when printed or displayed as there is no inherent risk of unauthorized access or disclosure. However, public information may require protections against a loss of integrity or availability. Confidential Information that is printed (e.g., spreadsheets, files, reports, presentations, and websites) should include the appropriate sensitivity label in the document footer on every printed page. Similarly, confidential information that is displayed (e.g. presentations) should also display the appropriate sensitivity label.

REFERENCES
The requirements established in the Security Categorization Policy have been derived from the following:

- NIST SP 800-53 Media Protection (MP), Access Control (AC), System and Communications Protection (SC), system and Information Integrity (SI), System and Service Acquisition (SA);
- NIST CSF Identify/Asset Management (ID.AM), Protect/Information Protection Policies and Procedures (PR.IP), Protect/Protective Technologies (PR.PT);
- NIST, Special Publication (SP) 800-60 Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories;
2006;

- NIST, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*


- HIPAA - 45 C.F.R. Part 164 Security and Privacy, and 42 USCS § 1320d-2 Standards for Information Transactions and Data Elements;

- Social Security Administration, *Data under the Computer Matching and Privacy Protection Act (CMPPA) of 1988* (Pub. L. No. 100-503) amended the Privacy Act to add several new provisions. See 5 U.S.C. § 552a (a)(8)-(13), (e)(12), (o), (p), (q), (r), (u) (2006); and

MEDIA PROTECTION (MP)

PURPOSE
The purpose of the Media Protection Policy is to ensure that data and information, in all forms and mediums, are protected throughout their lifecycles based on their security categorizations.

KEY TERMS
Access - Ability to make use of any information system or resource.

Data - A subset of information in an electronic format that allows it to be retrieved or transmitted.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Media - Physical devices or writing surfaces including, but not limited to: magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Sanitization - A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Portable Storage Device – is an information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Record – according to the State of New Jersey Open Public Records Act, P.L. 2001, CHAPTER 404 N.J.S. 47:1A-1 et seq., a "Government record" or "record" means any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, maintained or kept on file in the course of his or its official business by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by any such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof. The terms shall not include inter-agency or intra-agency advisory, consultative, or deliberative material.
According to N.J.S.A. 47:3-20, a "Record" or "records" means: pursuant to P.L. 1953, c.410, § 2 as amended by P.L. 1994, c.140, § 3 (N.J.S.A 47:3-16), any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound-recording or similar device, or any copy thereof which has been made or is required by law to be received for filing, indexing, or reproducing by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received by any such officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of the information contained therein.

**Sensitive Personally Identifiable Information (SPII)** - Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

**MP-01: POLICY**

Agencies shall implement appropriate processes and controls necessary to protect data and information in any medium or form (e.g. paper, magnetic media, tapes, portable devices, etc.) based on the data's sensitivity and criticality. Data must be protected during the system design, development, testing, implementation, and change processes to meet the Agency’s confidentiality and privacy commitments. Agencies are required to:

- (a) Maintain strict control over the storage and accessibility of media used to store information;
- (b) Properly maintain inventory logs of all media; and
- (c) Conduct media inventories at least annually.

This policy is supported by the following standards and guidelines.

**MP-02: SECURITY CATEGORIZATION**

Information System Owners in conjunction with Information Owners, Agency CISOs, Privacy Officers, and other key stakeholders are required to:

- (a) Categorize the information system and information; and
- (b) Document the security categorization results (including supporting rationale) for the information system.

Guidelines: The categorization of information and assets helps agencies to understand the potential adverse impacts on agency operations, agency assets, and individuals if agency information and information systems are comprised through a loss of confidentiality, integrity, or availability. Security categorization processes also facilitate the development of inventories of information assets and the controls necessary to adequately protect them.
MP-03: MEDIA STORAGE
Agencies shall implement controls to ensure the secure storage of digital and non-digital media. Agency management, asset custodians, and users and are required to:

(a) Physically secure all media;
(b) Maintain strict control over the storage and accessibility of media;
(c) Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility;
(d) Review the location’s security at least annually;
(e) Maintain strict control over the internal or external distribution of any kind of media, including the following:
   1. Categorize and label the media so the sensitivity of the information can be determined; and
   2. Send the media by secure delivery method that can be accurately tracked.

Guidelines: Controls for physically securing media are intended to prevent unauthorized persons from gaining access to sensitive information.

MP-04: SENSITIVE DATA INVENTORIES
Asset custodians and asset/process owners of sensitive information are required to:

(a) Maintain an inventory of all media on which sensitive information is stored;
(b) Where technically feasible, conduct periodic scans of information systems using automated tools to determine whether sensitive data (e.g., PII, PHI, payment card data, account credentials, etc.) is present on the system in clear text; and
(c) Conduct media inventories at least annually.

Guidelines: Using automated tools allows agencies to search for patterns (e.g. ###-##-####) that may indicate the presence of unprotected sensitive information that is susceptible to unauthorized access or disclosure. The OHSP Division of Cybersecurity maintains a site license for automated sensitive information discovery software that is available for use by agencies.

MP-05: CRYPTOGRAPHIC PROTECTION
Asset custodians and users are required to render sensitive data unreadable anywhere it is stored, including but not limited to, portable storage media, backup media, and in logs, by using technical measures including, but not limited to, strong cryptography with associated key-management processes and procedures. Sensitive data can be rendered unreadable through the means of:

(a) One-way hashes based on strong cryptography (hash must be of the entire sensitive data element);
(b) Truncation (hashing cannot be used to replace the truncated segment of the sensitive data element);
(c) Index tokens and pads (pads must be securely stored); or
(d) Strong cryptography with associated key-management processes and procedures.

Guidelines: Reference the Cryptographic Protection Policy and standards for cryptographic protection requirements.

**MP-06: MEDIA ACCESS**

Agencies shall implement controls and processes necessary to restrict access to digital and non-digital media to authorized individuals.

(a) Asset custodians and asset/process owners are required to assign Role-Based Access Controls (RBAC) to the specific data that is under their care to limit access to authorized personnel; and

(b) Sensitive Personally Identifiable Information (SPII) that is displayed or printed is required to be masked. This includes, but is not limited to:

(1) Financial account numbers;
(2) Social Security Numbers (SSN); and
(3) Credit or debit Primary Account Numbers (PANs).

Guidelines: Asset/Process owners and agency information security personnel should review Role-Based Access Controls (RBAC) on a quarterly basis to verify that only users with a business justification are able to access the data to which the controls provide access. Only personnel with a legitimate business need should be able to see the full SSN or PAN.

**MP-07: PORTABLE STORAGE DEVICES**

Agencies shall implement controls and processes to restrict the use of portable storage devices, and only authorize their use to individuals, devices, and endpoints where there is a justifiable business purpose, and the use is in compliance with internal agency policies, and all applicable State and Federal laws, and regulations. The following controls shall be implemented by all agencies, users, and asset custodians to protect sensitive information and mitigate the risks of system compromise as a result of the use of portable storage devices:

(a) Agencies shall:

(1) Maintain an inventory of all authorized portable storage devices; and

(2) Provide training to users of portable storage devices to ensure they are aware of the risks they pose, and that they are trained in how to implement cryptographic protections necessary to protect sensitive information.

(b) Users shall:
(1) Encrypt all sensitive information stored on a portable storage device using strong cryptography;
(2) Diligently protect the portable storage device from loss or theft;
(3) Immediately report lost or stolen portable storage devices; and
(4) Securely delete all sensitive information from portable storage devices when no longer necessary.

(c) Asset custodians shall:

(1) Disable the “Autorun” and “Autoplay” features on all endpoints; and
(2) Ensure anti-malware software is configured to perform real-time scans of all files from external sources as the files are downloaded, opened, or executed.

Guidelines: Portable storage devices are also commonly referred to as removable media. Portable storage devices introduce significant risk to the security of State information and information systems if their use is not sufficiently controlled. On highly sensitive and critical systems, agencies should consider disabling the connection ports used by portable storage devices in order to further reduce the risks of compromise of the systems. On other sensitive systems, agencies should consider limiting the types of devices that can be used. Whitelisting software and mechanisms can be implemented to allow for the connection of only authorized makes and models of portable storage devices.

Additional information and guidance on controlling the risks posed by the use of portable storage devices can be found in US CERT publication, The Risks of Portable Devices.

**MP-08: MEDIA TRANSPORTATION**

All users are required to ensure:

(a) Digital and non-digital media is protected during transport outside of agency-controlled areas;
(b) Accountability is maintained for system media during transport outside of agency-controlled areas; and
(c) Activities associated with transport of sensitive media are restricted to authorized personnel.

Guidelines: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, removable hard drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile computing and communications devices with information storage capability (e.g., laptop computers, smart phones and tablets) that are transported outside of agency-controlled areas.
MP-09: DATA LOSS PREVENTION
Where technically feasible, agencies shall deploy Data Loss Prevention (DLP) technologies to:

(a) Monitor for sensitive information (e.g., Sensitive Personally Identifiable Information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data; and

(b) Block such transfers while alerting information security personnel.

Guidelines: DLP strategies include implementation at the perimeter of the GSN via email and web content filtering technologies, as well as at individual agency endpoint (laptops, workstations, servers). The NJCCIC manages the Executive Branch’s enterprise mail filter solution that includes DLP capabilities. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.

MP-10: MEDIA SANITIZATION
Before disposal or re-use, media must be sanitized in accordance with the NIST Special Publication (SP) 800-88 rev. 1, Guidelines for Media Sanitization. These methods ensure that data is not unintentionally disclosed to unauthorized users.

Asset custodians and data/process owners are required to:

(a) Track, document, and verify media sanitization and disposal actions; and

(b) Periodically test sanitization equipment and processes used to sanitize digital media and document the results.

Guidelines: Media sanitization applies to all digital and non-digital media subject to disposal or reuse, to include media found in devices such as scanners, copiers, and printers. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed.

The sanitization method to be used depends on the type of storage media, the sensitivity of the information which it stores, and the purpose of the media after it is sanitized.

There are three primary methods for sanitizing storage media:

**Clearing** – refers to the method of sanitizing media by overwriting user addressable storage space on the media with non-sensitive data. When media is sanitized using the clearing method it is infeasible that the cleared data will be recoverable using commercially available data recovery tools.

**Purging** – refers to a stronger method of sanitization that protects the sanitized data from recovery even when using advanced laboratory techniques. Some methods of purging - such as the degaussing of magnetic media - will render the media unusable afterwards, whereas purging by the use of a firmware secure erase command will sanitize the media and allow for its reuse.
Destroying – refers to the physical destruction of the media rendering the data unrecoverable. Acceptable methods of destruction include:

- Disintegration, pulverization, melting, and incineration which will completely destroy the media and any data it contains; or
- Shredding - The shred size of the refuse should be small enough to provide reasonable assurance that the data cannot be reconstructed.

**MP-11: RECORDS RETENTION**

Agencies shall implement records retention programs within their respective agencies to ensure records (e.g. data and information) are retained in accordance with the State of New Jersey, Chapter 410, Laws of 1953, Destruction of Public Records Act, the State General Records Retention Schedule, other applicable State and Federal Laws, litigation holds, regulations, and agency business requirements.

The storage of sensitive information that has no business value, and for which all retention requirements have expired, introduces unnecessary risks and is to be disposed of in accordance with the Media Sanitization requirements contained herein. Agencies’ data retention programs shall be designed to provide for the systematic retention and destruction of physical and digital records based on statutory and regulatory record-keeping requirements and business needs that include:

(a) Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements;

(b) Processes for secure deletion of data when no longer needed; and

(c) A regular process (automatic or manual) for identifying and securely deleting stored sensitive data that exceeds defined retention requirements.

Guidelines: The retention of data (e.g., paper documents, backup tapes, email messages and other media) not otherwise necessary to conduct business or needing to be retained for legal purposes, is both expensive and inefficient.

**MP-12: DISPOSAL**

Storage media and hard copy records are to be disposed/destroyed using formal processes and procedures appropriate with the information’s sensitivity, and in accordance with the State and Federal retention requirements. For more information on State of New Jersey retention schedules please visit: [http://www.nj.gov/treasury/revenue/rms/retention.shtml](http://www.nj.gov/treasury/revenue/rms/retention.shtml).

**REFERENCES**

The requirements established in the Media Protection Policy have been derived from the following:

- NIST SP 800-53 Media Protection (MP), Access Control (AC), System and Communications Protection (SC); and
• NIST CSF Identify/Asset Management (ID.AM), Protect/Information Protection Policies and Procedures (PR.IP), Protect/Protective Technologies (PR.PT).
CRYPTOGRAPHIC PROTECTION (CR)

PURPOSE
The purpose of the Cryptographic Protection Policy is to ensure the confidentiality of sensitive information through the implementation of cryptographic technologies.

KEY TERMS
Cipher - Series of transformations that converts plaintext to ciphertext using the Cipher Key.

Cryptography - Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography that makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret.

Decryption - The process of changing ciphertext into plaintext using a cryptographic algorithm and key.

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Hashing - The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Interface - A shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these factors.

Non-Console Access - Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.

Plain Text - Information that is not encrypted.

Strong Cryptography - Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is “one way”; that is, not reversible). See Hashing.

At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC
(224 bits and higher), and DSA/D-H (2048/224 bits and higher). Strong cryptography is also commonly referred to as a strong encryption.

**CR-01: POLICY**

Agencies shall employ cryptographic safeguards to protect sensitive information in transmission, in use, and at rest, from a loss of confidentiality, unauthorized access, or disclosure. The use of cryptographic protection technologies shall comply with all applicable State and Federal laws, regulations, contractual requirements, and internal agency policies.

This policy is supported by the following standards and guidelines

**CR-02: USE OF CRYPTOGRAPHIC CONTROLS**

Asset custodians, in conjunction with asset owners, are required to establish and implement processes and technical measures for the use of encryption protocols for protection of sensitive information at rest (e.g., file servers, databases, and end-user workstations), in use (memory), and in transit (e.g., system interfaces, over public networks, and electronic messaging) in accordance with applicable State and Federal statutory and regulatory compliance requirements, contractual obligations, and internal agency policies. This includes, but is not limited to:

(a) Employing platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms;

(b) Using strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;

(c) Verifying that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices;

(d) Verifying that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations; and

(e) Separating key management and key usage duties.

Guidelines: Various State and Federal statutes and regulations require the encryption of sensitive information, including, but not limited to, Federal Tax Information (FTI), medical records, payment card numbers, Criminal Justice Information (CJI), etc. Agencies should review the data types they use to ensure compliance with all applicable laws and regulations regarding cryptographic protection obligations.

Agencies should refer to NIST Special Publication (SP) 800-175B *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* for guidance on the selection and implementation of cryptographic controls based on the security categorization and risk environment of the data and/or information system.

**CR-03: ENCRYPTION ALGORITHMS**
 Agencies shall ensure that all encryption algorithms used to protect sensitive information meet Federal Information Processing Standards (FIPS) 140-2 cryptographic module validation requirements. FIPS 140-2 approved security functions include:

- Advanced Encryption Standard (AES); and
- Triple Data Encryption Standard (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA).

For hashing, the Secure Hash Standard (SHS) Secure Hash Algorithm (SHA) family of algorithms (SHA-224, SHA-256, SHA-384 and SHA-512) and SHA3 are approved.


**CR-04: ENCRYPTION OF DATA IN TRANSIT**

To protect the confidentiality and integrity of information in transit, asset custodians and asset owners are required to:

- (a) Implement strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;
- (b) Ensure only trusted keys and certificates are accepted;
- (c) Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices; and
- (d) Verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.

Guidelines: The requirement for the use of encryption of data in transit applies to both internal and external networks. Over the past several years, vulnerabilities in earlier versions of cryptographic protocols (e.g. SSL, TLS) have rendered them insecure. Laws and regulations governing the use of cryptographic protocols require that agencies implement the latest supported versions.

Agencies must ensure that there is end-end protection of data in transit between the system components/services originating the transmitted information and the system components/services receiving the transmitted information. Agencies should refer to NIST Special Publication (SP) 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations for additional guidance on the use of cryptographic protocols to be used to protect data in transit.
Agencies should refer to the Security for Publicly Accessible Web Sites and Services Policy for further information on the required use of HTTPS for all publicly accessible web sites and services.

**CR-05: CRYPTOGRAPHIC PROTECTION OF DATA AT REST**

Asset owners, asset custodians, and users shall ensure information stored on agency information assets are protected by employing cryptographic protection mechanisms in accordance with the sensitivity of the information and the categorization of the system, and all applicable State and Federal laws, regulations, contractual requirements, and internal agency policies.

Guidelines: This requirement addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. This standard also applies to backup media, portable storage devices, portable computing and communications devices (e.g. laptops, smartphones, tablets, etc.).

System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Agencies may employ different mechanisms to achieve confidentiality and integrity protections. Agencies may also employ other security controls including, for example, secure off-line storage in lieu of online storage, when adequate protection of information at rest cannot otherwise be achieved.

**CR-06: CRYPTOGRAPHIC PROTECTION FOR AUTHENTICATORS**

Asset custodians and asset owners are required to ensure all information systems, applications, and databases use strong cryptography to render all passwords unreadable during transmission and storage on all information system components.

Guidelines: The transmission and storage of authenticators (e.g. passwords) must be protected using strong cryptography. The unauthorized access or disclosure of authenticators could severely adversely impact the confidentiality, integrity, availability, and privacy of information and information systems.

**CR-07: NON-CONSOLE ADMINISTRATIVE ACCESS**

Asset custodians shall ensure all non-console administrative access to agency systems use strong cryptography and secure protocols (e.g. VPN, TLS, SSH). The use of insecure protocols (e.g. Telnet) is not permitted. Asset custodians are responsible for developing configuration standards to ensure all non-console administrative access is encrypted using strong cryptography, utilizing technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.

Guidelines: Non-console access includes access from within local/internal networks as well as access from external, or remote, networks. In addition to the strong cryptography and secure protocol requirements, all non-console administrative access shall require the use of multi-factor...
authentication in accordance with the Identity and Authentication Management Policy included in this Manual.

**CR-08: WIRELESS ACCESS AUTHENTICATION AND ENCRYPTION**
Asset owners and asset custodians are required to ensure wireless networks employ industry-recognized leading practices to implement strong encryption for authentication and transmission.

Guidelines: Asset owners and asset custodians should refer to the Center for Internet Security (CIS) Benchmarks and vendor documentation for the proper security configurations of Wireless Access Points (WAPs) and supported encryption strength.

**CR-09: CRYPTOGRAPHIC KEY MANAGEMENT**
Asset custodians are required to implement administrative and technical measures to protect keys used to secure sensitive information against disclosure and misuse, including the following:

(a) Maintain a documented description of the cryptographic architecture that includes:
   (1) Details of all algorithms, protocols, and keys used for the protection of sensitive information, including key strength and expiry date;
   (2) Description of the key usage for each key; and
   (3) Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management;

(b) Cryptographic key access shall be restricted to the fewest number of custodians necessary;

(c) Cryptographic keys shall be securely stored at all times using one of the following methods:
   (1) Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key;
   (2) Within a secure cryptographic device (such as a host security module (HSM)); or
   (3) As at least two full-length key components or key shares, in accordance with an industry-accepted method;

(d) Cryptographic keys must be securely stored in the fewest possible locations and forms;

(e) Asset custodians are required to document and implement key management processes and procedures for cryptographic keys used for encryption of sensitive information that includes the following:
   (1) Procedures for the generation, distribution, and storage of keys;
   (2) Generation of strong cryptographic keys;
   (3) Prevention of unauthorized substitution of cryptographic keys;
(4) Distribution of cryptographic keys using secure methods; and
(5) Secure storage of cryptographic keys;

(f) Changing cryptographic keys that have reached the end of their cryptoperiod:
   (1) After a defined period of time has passed and/or after a certain amount of cipher-
       text has been produced by a given key;
   (2) As defined by the associated application vendor or key owner; or
   (3) Based on industry-recognized leading practices and guidelines (e.g., NIST Special
       Publication (SP) 800-57, Recommendation for Key Management);

(g) Retiring or replacing keys when the integrity of the key has been weakened or the keys
    are suspected of being compromised:
   (1) Retiring or replacing may be performed by archiving, destruction, and/or
       revocation of keys; and
   (2) Keys should be considered compromised by the departure of an employee with
       knowledge of a clear-text key;

(h) Split knowledge and dual control, if manual, clear-text cryptographic key management
    operations are used. If applicable, these operations require procedures that require two
    or three people, each knowing only their own key component, to reconstruct the whole
    key;

(i) Requiring cryptographic key custodians to formally acknowledge that they understand
    and accept their key-custodian responsibilities.

Guidelines: The management of cryptographic keys leaves little room for error. The loss or
compromise of encryption keys can result in a complete loss of authorized access to agency data
or a compromise of agency data. Individuals who are as assigned key custodians on behalf of the
agency must be aware of their unique roles. Agencies should perform due diligence to ensure
key custodians have the required skills, knowledge, and trustworthiness. Criminal background
checks should be performed, in accordance with all applicable State and Federal laws, on
individuals in agency key custodian positions.

Additionally, ensuring availability of cryptographic keys used for encryption of data at rest is
critical. Lack of access to the cryptographic keys will not allow the decryption of the data causing
the encrypted data to be unavailable.

Note: Encryption keys used for encryption and decryption should not be used for digital
signatures.

**CR-10: SYMMETRIC AND ASYMMETRIC KEYS**
Where technically feasible:

   (a) Agencies shall produce, control, and distribute symmetric cryptographic keys using FIPS-
       compliant key management technology and processes; and
(b) Agencies shall produce, control, and distribute asymmetric cryptographic keys using approved key management technology and processes that protect the user’s private key.

REFERENCES

The requirements established in the Cryptographic Protection Policy have been derived from the following:

- NIST SP 800-53 Access Control (AC), System and Communications Protection (SC), Identity and Authentication (IA); and
- NIST CSF Protect/Data Security (PR.DS); Protect/Access Control (ID.AC).
PURPOSE
The purpose of the Access Management Policy is to establish the security requirements and ensure the appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, State information assets.

KEY TERMS
Access - Ability to make use of any information system or resource.

Authenticator - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Identifier - Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers.

Least Privilege - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. Least privilege is also the security objective of granting users only those accesses they need to perform their official duties.

AC-01: POLICY
Agencies shall establish procedures that effectively control and restrict access to agency information assets to authorized users based on defined business and legal requirements (essentially, access will be limited to a “need-to-use” and/or “need-to-know” basis). Mechanisms are required to be implemented that provide for the control, administration, and tracking of access to, and the use of, agency information assets, as well as the protection of such assets from unauthorized or unapproved activity and/or destruction.

This policy is supported by the following standards and guidelines.

AC-02: ROLE BASED ACCESS
User access to information assets shall be applied according to an individual’s role and business requirements for such access. All information stored on agency information systems shall be protected with the file system, network share, claims, application, or database specific access control lists. These Role-Based Access Controls (RBAC) will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their job responsibilities.

Guidelines: Agencies are to define roles according to a user’s job competency, authority, and responsibility within the agency.
AC-03: PRINCIPLE OF LEAST PRIVILEGE

Agencies shall employ the principle of least privilege in order to limit access to the minimal level users require to carry out their duties and responsibilities.

(a) Authorized individuals performing functions requiring privileged access must use designated privileged accounts only for administrative activities and use standard user accounts for all other purposes; and

(b) The principle of least privilege is also to be applied to programs and processes.

Guidelines: The concept of least privilege is to be applied for specific duties and information systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions.

AC-04: SEGREGATION OF DUTIES

The principle of segregation of duties is to be adhered to when assigning functions, tasks, and responsibilities for critical business processes, system maintenance, day-to-day computer operations, and security/system administration. Specifically, the concept of segregation of duties is to ensure that:

(a) Individuals who request authorization to carry out a task are distinct and separate from those who approve the request;

(b) Test functions are performed separately from production and development functions;

(c) Auditing functions are distinct and separate from the function implementing the controls;

(d) Individuals assigned to an information security role are not also assigned to an information systems role; and

(e) Database developers do not perform the functions of a database administrator.

AC-05: USER ACCOUNT MANAGEMENT

Agencies are responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion, and modification of User-IDs, credentials, and other identifier objects to ensure authorized use is maintained;

(b) Verify user identity before issuing initial passwords or performing password resets;

(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;

(d) Immediately revoke access for any terminated users;

(e) Remove disabled user accounts within ninety (90) days;
(f) Limit repeated access attempts by locking out the User-ID after more than five (5) failed attempts;

(g) Set the lockout duration to a minimum of thirty (30) minutes or until an administrator unlocks the User-ID;

(h) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;

(i) Enable accounts used by vendors for remote access only during the time period needed, and monitor vendor remote access accounts when in use;

(j) Disable or remove default User-IDs and accounts;

(k) Restrict user direct access or queries to databases only to database administrators, including:

(1) Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);

(2) Verify that database and application configuration settings restrict user direct access or queries to databases only to database administrators; and

(3) Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes;

(l) Establish methods to limit or restrict concurrent sessions in order to provide reasonable assurances that only an authorized user of an information asset has gained authorized access.

Guidelines: Agencies should review access privileges granted to users every six (6) months to determine if access rights are commensurate with the user’s job duties. Evidence of account and privilege reviews that document the review occurred, who conducted the review, and what action (if any) was taken should be maintained for a period of twelve (12) months.

**AC-06: REQUIREMENTS FOR ACCOUNT REGISTRATION AND CREATION**

Agencies shall establish and document formal account creation and registration processes to include the following:

(a) Agencies shall ensure that each User-ID generated is unique;

(b) User-IDs should be granted to specific users only, and should not be used by anyone but the individuals to whom they have been issued;

(c) The use of group accounts and shared IDs is generally prohibited. The use of such accounts shall require prior approval by the agency Chief Information Security Officer or his/her delegate;
(d) The creation of an individual user account shall require a written or electronic request from an appropriate authorized manager, and/or Human Resources representative;

(e) Access to information assets, systems and services shall be provided in accordance with a user’s job description/function/role on a “need-to-know” and/or “need-to-use” basis (access should correspond to the minimum amount of privilege necessary for an individual user’s proper job function/duties/requirements and not necessarily their job title);

(f) User-ID’s shall not give any indication of the user’s privilege level (i.e., Administrator);

(g) User accounts should be created in such a way as to facilitate their periodic review by the Agency information security personnel and asset custodians;

(h) Access control rules and rights for each user or group of users shall be defined and documented;

(i) Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

(j) The initial authentication factor (password) shall be valid only for the user’s initial login to the system or application;

(k) The user account shall be disabled if the initial password is not used within thirty (30) days;

(l) The user shall be forced to change the password before completion of the initial login sequence; and

(m) Before any third-party vendor or contractor is given access to Agency information assets, a contract defining the terms and conditions of such access should be signed by the third-party vendor or contractor.

**AC-07: REQUIREMENTS FOR PRIVILEGED ACCESS**

Agencies shall restrict and control the allocation and use of privileged user accounts.

(a) Privileged accounts shall be limited to the minimum number required for successful management and operation of the agency information systems;

(b) The allocation of privileged access shall be provided on a “need-to-use” and/or “need-to-know” basis (privileges should correspond to the minimum amount of privilege necessary for an individual user’s proper job function/duties/requirements and not necessarily their job title);

(c) The process for granting privileged access shall follow the same requirements as the user registration process;

(d) Privileged access shall be used only for duties that require escalated privileges;

(e) Privileged access shall be audited and logged at all times;
(f) Privileged access shall be protected and granted in such a way as to ensure that actions conducted while using privileged access can be traced to a unique user account; and

(g) Where technically feasible, or otherwise required by policy, Executive Order, statutory, regulatory, or contractual requirement, advanced authentication methods such as multi-factor authentication, biometrics, etc., are to be used for privileged access accounts.

Guidelines: Privileged access is defined as a level of access above that of a normal user and is commonly reserved for the administration of a system, device, application, database or other such information asset. Privileged accounts are also commonly referred to as Administrator, Admin, Root, and Super User accounts.

**AC-08: REQUIREMENTS FOR TEMPORARY OR EMERGENCY ACCESS**
Temporary or emergency accounts may be established by Agencies to support specific business functions for which such access is required.

(a) Agencies shall develop procedures to properly authorize temporary or emergency access accounts, including documenting their creation and deletion when no longer needed; and

(b) Agencies shall apply password and authentication controls for temporary and emergency accounts commensurate with the role – user or administrator – required by the Identification and Authentication Policy as documented in this Manual and in accordance with other policy, contractual, and statutory requirements. Any deviation from the password and authentication requirements shall require approval by the Agency Information Security Officer.

**AC-09: USER ACCOUNT LOCK OUT AND SUSPENSION**
Users attempting to use/access agency information assets, systems, and networks must identify themselves individually via a secure logon procedure. In order to reduce the risk of a malicious user or program using a brute force attack or a continuous process to access agency resources, the following shall be adhered to:

(a) All user accounts shall be locked out after five (5) unsuccessful access attempts. As a result of unsuccessful attempts, the system should log the attempts with time, date, and location and force a time-delay before allowing further logon attempts;

(b) Inactive User IDs shall be disabled after sixty (60) days of non-use;

(c) Suspended and/or locked user accounts shall require a system administrator to unlock the account;

(d) Users with appropriate access may use an authorized agency password maintenance application to unlock their account using a personalized security question and answer system or other means of authentication, as approved by the Agency Information Security Officer or an authorized designee;
(e) Users with appropriate access may utilize a system that provides a process to automatically unlock an account after a predetermined period of time. The respective system or application owner must authorize systems of this nature; and

(f) The agency or individual sponsoring a third-party user who is not a State employee shall be responsible for informing the third-party organization of its responsibility for timely notification of terminated users.

**AC-10: SESSION LOCK**

Agencies shall ensure systems are configured to prevent access to the system:

(a) After receiving a manual command from the user to implement a session lock; and

(b) Automatically implementing a session lock after fifteen (15) minutes of inactivity.

Guidelines: Session locks are temporary actions taken to prevent further access to an information system until the user re-authenticates to the system. Upon activation of a session lock the contents of the screen are hidden from view and access to the system is halted. Typically, screen savers are displayed upon the activation of a session lock.

**AC-11: MANAGEMENT OF USER ACCOUNTS AND ACCESS**

Access to agency information assets shall be controlled through the following formal user management process:

(a) Access control rules and rights for each user, or group of users, shall be clearly documented;

(b) All user access creation, deletion, and other privilege change activity shall be reviewed periodically by the Agency CISO or a designee;

(c) Accounts that are inactive beyond sixty (60) days shall be disabled;

(d) A formal account de-registration process shall be established to remove terminated accounts from Agency systems;

(e) Access rights for users who have changed roles shall be reviewed and modified based on their new job description and need-to-know, before being reinstated;

(f) Upon user transfer or termination, the Agency shall immediately remove, revoke or change user account access rights, as appropriate; and

(g) Any suspension or termination of an individual’s access rights/privilege shall be immediately reported to Agency CISO.

**AC-12: SUSPENSION OF ACTIVE ACCOUNTS**

In certain instances, it may be necessary to temporarily suspend access for individuals who have an active status. In those instances, access shall be suspended unless the Agency Human Resources representative authorizes in writing or electronic form that the user’s access should be maintained. Those instances include, but are not limited to, the following:
(a) Leave of Absence:
   (1) Short-term disability;
   (2) Long-term disability;
   (3) Military leave; or
   (4) Other authorized leave;
(b) Terminations:
   (1) User terminations are divided into the following three (3) categories:
   (2) Voluntary termination;
   (3) Involuntary termination; or
   (4) Third-party vendor or contractor termination;
(c) In the event of a termination, the following shall be adhered to:
   (1) For terminations, both voluntary and involuntary, the Agency Human Resources
       representative shall be involved in the notification process;
   (2) For terminations, both voluntary and involuntary, the Agency Human Resources
       representative shall immediately notify all appropriate parties;
   (3) Upon appropriate notification, all responsible administrators shall immediately
       disable permission granting the subject user’s access to agency information assets;
       and
   (4) For contractor or other third-party user terminations, the third-party vendor or
       organization shall be responsible for immediate notification to the agency;
(d) Emergency Suspension of Active Accounts:
   For exigent circumstances in which there is a real or perceived threat to the safety,
   security or privacy of persons or property, including State of New Jersey information
   assets, managers are authorized to bypass the Human Resources notification
   requirement in order to immediately suspend a user’s account. Requests for emergency
   suspensions will be documented and Human Resources will be notified post-suspension,
   as appropriate.

**AC-13: SYSTEM USE NOTIFICATION**

Where technically feasible, asset custodians are to configure State information systems to display
an agency-defined system-use notification banner that is displayed to users before granting
access to the system. The notification banner shall include privacy and security notices consistent
with applicable Federal and State laws, Executive Orders, directives, policies, regulations,
standards, and guidance and shall:

(a) State the following:
   (1) Users are accessing an information system owned by the State of New Jersey;
(2) Information system usage may be monitored, recorded, and subject to audit;

(3) Unauthorized use of the State information system is prohibited and subject to criminal and civil penalties; and

(4) Use of the State information system indicates consents to monitoring and recording.

(b) Retain the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to, or further access the State information system.

Guidelines: An example of a logon banner that may be used includes the following:

This is a State of New Jersey information system which may be accessed and used only for official government business by authorized personnel. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative action. Administrative action may include discipline, up to and including, termination of employment or contract. All information on this system may be intercepted, recorded, read, copied, or disclosed by, and to, authorized personnel for official purposes, including, criminal, civil and/or administrative investigations. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.

AC-14: PERIODIC REVIEW

Agencies shall document and implement a formal process to periodically review users’ access rights in order to maintain effective controls over user access to information assets. To maintain these effective controls, agencies are required to:

(a) Review user access to resources at least every six (6) months. The review should specifically identify and revoke access for, or remove, the following:

(1) Active User-IDs that are no longer needed;

(2) User-IDs assigned to terminated users with active access;

(3) Generic or anonymous User-IDs that are no longer needed;

(4) Redundant or duplicate User-IDs;

(5) User-IDs with excessive privileges, which are no longer necessary and/or are not approved; and

(6) Maintain evidence that documents the reviews were completed;

(b) Establish procedures to monitor the events and activities of each user accessing agency systems, networks and information assets to detect deviations from authorized use; and

(c) Establish controls to ensure that logon activity is monitored and logged to a centralized log management system.
REFERENCES

The requirements established in the Access Management policy have been derived from the following references:

- NIST SP 800-53: Access Controls (AC); Identity and Authentication (IA); and
- NIST CSF: Protect – Access Control (PR-AC).
IDENTITY AND AUTHENTICATION (IA)

PURPOSE
The purpose of the Identity and Authentication Policy is to establish the identification, authorization, and authentication requirements necessary to ensure access to State information assets is controlled and securely provided to only authorized individuals, systems, and processes.

KEY TERMS
Access - Ability to make use of any information system or resource.

Authenticator - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Identifier - Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers.

Least Privilege - The security objective of granting users only those accesses they need to perform their official duties.

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Multi-factor Authentication - Authentication using two or more factors to achieve authentication. Factors include:

(i) something you know (e.g. password/PIN);
(ii) something you have (e.g., cryptographic identification device, token); or
(iii) something you are (e.g., biometric). See Authenticator.

Public Key Infrastructure (PKI) - A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

SensitivePersonally Identifiable Information (SPII) – is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

IA-01: POLICY
Agencies shall establish procedures and implement identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access State of New Jersey information and information systems.
This policy is supported by the following standards and guidelines.

**IA-02: PRINCIPLE OF LEAST PRIVILEGE**

Agencies shall employ the principle of least privilege in order to limit access to the minimal level users require to carry out their duties and responsibilities.

(a) Authorized individuals performing functions requiring privileged access must use designated privileged accounts only for administrative activities and use standard user accounts for all other purposes; and

(b) The principle of least privilege is also to be applied to programs and processes.

Guidelines: The concept of least privilege is to be applied for specific duties and information systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions.

**IA-03: IDENTIFICATION AND AUTHENTICATION**

Agencies shall ensure agency information systems uniquely identify and authenticate users (or processes acting on behalf of users).

Agencies are required to assign each user a unique identification (User-ID) before allowing them to access systems. In addition to assigning a unique User-ID, employ at least one (1) of the following methods to authenticate all users:

(a) Something you know, such as a password or passphrase;

(b) Something you have, such as a token device or smart card; or

(c) Something you are, such as a biometric.

**IA-04: USER PROVISIONING AND DEPROVISIONING**

Agencies shall document, implement and manage a formal user access provisioning process to assign and/or revoke access rights for all user types, to all systems and services.

Guidelines: Provisioning user access to data and State-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the agency's management prior to access being granted.

Timely de-provisioning (revocation or modification) of user access to information and State-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented. Revocation or modification of access is often required when there is a change in the user's status (e.g., termination of employment or contract, job reassignment, or transfer).
**IA-05: ROLE BASED ACCESS CONTROL**

User access to information assets shall be applied according to an individual’s role and business requirements for such access. All information stored on agency information systems shall be protected with the file system, network share, claims, application, or database specific access control lists. These Role-Based Access Controls (RBAC) will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their job responsibilities.

Guidelines: Agencies are to define roles according to a user’s job competency, authority, and responsibility within the agency.

**IA-06: USER ACCOUNT MANAGEMENT**

Agencies are responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion, and modification of User-IDs, credentials, and other identifier objects to ensure authorized use is maintained;

(b) Verify user identity before issuing initial passwords or performing password resets;

(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;

(d) Immediately revoke access for any terminated users;

(e) Remove disabled user accounts within ninety (90) days;

(f) Limit repeated access attempts by locking out the User-ID after more than five (5) failed attempts;

(g) Set the lockout duration to a minimum of thirty (30) minutes or until an administrator unlocks the User-ID;

(h) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;

(i) Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;

(j) Minimize the use of group, shared, or generic accounts and passwords;

(k) Disable or remove default User-IDs and accounts;

(l) Restrict user direct access or queries to databases only to database administrators, including:

   (1) Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);

   (2) Verify that database and application configuration settings restrict user direct access or queries to databases only to database administrators; and
(3) Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

(m) Establish methods to limit or restrict concurrent sessions in order to provide reasonable assurances that only an authorized user of an information asset has gained authorized access.

Guidelines: Agencies should review access privileges granted to users every six (6) months to determine if access rights are commensurate with the user’s job duties. Evidence of account and privilege reviews that document the review occurred, who conducted the review, and what action (if any) was taken should be maintained for a period of twelve (12) months.

**IA-07: IDENTIFIER MANAGEMENT**

Agencies are required to ensure proper identification management for all user accounts.

(a) Ensure that only authorized users are provided with User-IDs;

(b) Ensure that each user name that is generated is unique and created in a manner that is consistent with agency defined User-ID naming conventions;

(c) Ensure that each User-ID provides no insight into the user’s privilege (e.g. Admin, Administrator);

(d) Require written or electronic authorization by a supervisor or manager to receive or create a User-ID;

(e) Prevent the reuse of identifiers for one year;

(f) Prohibit anonymous access to any agency information systems unless the system is designed for all users to be anonymous; and

(g) Limit the use of group, shared, or generic account identifiers and authentication methods.

Guidelines: Systems that may allow for anonymous access include web sites, intranet sites, bulletin boards, etc.

Generic and shared accounts are generally prohibited on devices, systems, and solutions used to conduct agency business processes. In those situations, when a generic or shared account is created, it is required to be restricted to provide the minimal amount of access necessary to carry out the business function.

**IA-08: AUTHENTICATOR MANAGEMENT**

Agencies shall implement processes that manage authenticators (e.g. passwords, tokens, biometrics, PKI certificates, and key cards) for users and devices as follows:

(a) Verify, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
(b) Ensure that authenticators have sufficient strength of mechanism for their intended use;
(c) Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
(d) Change default authenticators upon system installation;
(e) Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
(f) Change/refresh authenticators according to a agency-defined time period by authenticator type;
(g) Protect authenticator content from unauthorized disclosure and modification; and
(h) Require users to take, and have devices implement, specific measures to safeguard authenticators.

Guidelines: Authenticators include, but are not limited to, passwords, tokens, biometrics, PKI certificates, and key cards. The strength of mechanism of an authenticator is dependent on a number of factors including the composition, lifetime, length, and protection of the authenticator from disclosure. Specific actions to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.

In many cases, vendors ship products with factory default authenticators (passwords) to allow for initial installation and configuration. Default passwords are often well known, easily discoverable, and present a significant security risk if left unchanged.

**IA-09: MULTI-FACTOR AUTHENTICATION (MFA)**

Multi-factor authentication shall be required for the following:

(a) Network access to privileged accounts;
(b) Remote network access originating from outside an agency’s network;
(c) Non-console (network) access for personnel with administrative access to sensitive information or systems;
(d) As technically feasible, agencies shall require multi-factor authentication for local access to privileged accounts; and
(e) Where multi-factor authentication is not supported for local access to privileged accounts, accounts must use at least fifteen (15) character passwords.

Guidelines: Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods. Examples of multi-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system
(TACACS) with tokens; and other technologies that facilitate multi-factor authentication. Using one factor twice (e.g., using two separate passwords) is not considered multi-factor authentication.

**IA-10: MULTI-FACTOR AUTHENTICATION – SEPARATE DEVICE**

Agencies shall ensure that agency information systems for which multifactor authentication is required for remote access, requires that one of the factors is provided by a device separate from the system to which remote access is being made, and that the device meets cryptographic standards for strength of mechanism in accordance with the Cryptographic Protection Policy.

**IA-11: PASSWORD AUTHENTICATION MANAGEMENT**

Agencies shall document and implement processes that require that the passwords for all accounts provided to authorized users, be managed to the extent that use of said password provides reasonable assurance that the individual logging on is the individual to whom the account is assigned. Password authentication management requirements include the following:

(a) **Restrictions on Password Sharing**: All users shall be prohibited from sharing, revealing, or otherwise disclosing individual password information;

(b) **Restrictions on Requesting Password Information**: Agency personnel shall be prohibited from requesting password information from others;

(c) **Restrictions on Passwords in Scripts**: Agency personnel, including contractors or those employed by contracted entities, are prohibited from embedding passwords in scripts or within other workflow situations in which the password is retained in clear text;

(d) **Requirements for Storing Password Information**: Passwords are not to be stored in a human readable format or in a location where an unauthorized individual might discover them. When password storing is required, electronic passwords are to be stored an encrypted format. Hard copy or written passwords are to be stored in a secured location;

(e) **Restrictions on Displaying Passwords**: Personnel are prohibited from displaying passwords. Agency information systems that require passwords shall mask, suppress, or otherwise obscure the password upon entry to prevent unauthorized disclosure;

(f) **Restrictions on Password Communication**: Communication of passwords is an essential part of ensuring that appropriate authorization occurs for agency personnel when they access information resources;

(g) **Restrictions on Authorized Password Recipients**: The identified owner of an account is the only person authorized to receive password information;

(h) **Restrictions on Initial Password Communication**: Initial passwords are to be communicated directly to the identified owner of an account. However, when password disclosure to the identified account owner is not possible, passwords may be communicated to another employee at the discretion of the account owner’s supervisor. This password will be configured to expire on first use, as required by this standard; and
(i) **Requirements for Initial or Reset Passwords:** Initial or reset passwords provided to, or received by, the account’s owner will expire upon first use, thus requiring the account owner to change the password at first use. Initial or reset passwords will be configured to provide suitable strength of mechanism while still following the password composition requirements as described below.

**IA-12: PASSWORD REQUIREMENTS FOR STANDARD USER ACCOUNTS**

Agencies shall establish authentication and password requirements that meet at least the following minimum requirements for individual user accounts used to authenticate to agency information assets. More restrictive controls may be implemented based upon the sensitivity and criticality of the information asset, or other policy, statutory, regulatory, and contractual requirements.

(a) Passwords for individual user accounts are required to be at least eight (8) characters in length;

(b) Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters;

(c) Passwords are required to contain characters from each of the following four categories:
   
   (1) English uppercase characters (A through Z);
   
   (2) English lowercase characters (a through z);
   
   (3) Base 10 digits (0 through 9); and
   
   (4) Non-alphanumeric characters (for example: !, $, #, >, %).

(d) Users shall be required to change their passwords at least every 90 days or immediately upon the suspected compromise of the password;

(e) Systems shall be configured to prohibit users from changing their passwords more than once in a 24-hour period. If it is necessary for a user to change a password more than once within a 24-hour period, the user will be required to contact the Agency’s IT Service Desk for assistance; and

(f) Users shall be restricted from reusing their previous 24 passwords.

**Guidelines:** Passwords may exceed 8 characters so long as agency business processes are not negatively impacted. Passwords should never be written down or stored on-line in an unencrypted format. Users must create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, for a standard user account the phrase: "Tramps like us, baby we were born to run" may be used to create an easily remembered password: "Tlu,bwwb2r" that meets all complexity requirements.
Strong (good) passwords have the following characteristics:

- Contain both upper and lowercase characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*);
- Have eight (8) or more alphanumeric characters;
- Are not a word in any language, slang, dialect, or jargon; and.
- Not based on personal information, names of family members, or important calendar dates.

Weak (bad) passwords have the following characteristics:

- Default vendor password;
- Contain less than eight (8) characters;
- A word found in a dictionary (English or foreign);
- A common usage word such as: Names of family members, pets, etc.;
- Birthdays and other personal information such as addresses and phone numbers;
- Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts or 123321);
- Any of the above spelled backward; and/or
- Any of the above preceded or followed by a digit (e.g., password1 or 1password).

In June of 2017, NIST published Special Publication (SP) 800-63-3: Digital Authentication Guidelines that provides new guidance regarding passwords. Most significantly, the guidelines remove the complexity requirement for passwords and instead focuses on password strength based on its length as an indicator of strength. The longer a password, the more entropy it has, and mathematically it will take longer to brute force guess the password. While the NIST guidelines remove the complexity requirement for passwords, the State of New Jersey password requirements shall continue to include the complexity requirement to satisfy its compliance obligations with statutory, regulatory, and contractual requirements regarding authentication.

**IA-13: PASSWORD REQUIREMENTS FOR ADMINISTRATIVE ACCOUNTS**

Administrative accounts are defined as user accounts with privileged access and are commonly used for the administration of a system, device, application, database or other such information asset.

(a) As technically feasible, passwords for administrative accounts are required to be at least fifteen (15) characters in length;

(b) Passwords shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters;

(c) Passwords are required to contain characters from each of the following four categories:
(1) English uppercase characters (A through Z);
(2) English lowercase characters (a through z);
(3) Base 10 digits (0 through 9); and
(4) Non-alphanumeric characters (for example: ! $ # > %);
(d) Users of administrative accounts shall be required to change their passwords at least
every 45 days or immediately upon the suspected compromise of the password;
(e) Systems shall be configured to prohibit users with administrative privileges from changing
their passwords more than once in a 24-hour period. If it is necessary for a user with
administrative privileges to change a password more than once within a 24-hour period,
the user will be required to contact the Agency’s IT Service Desk for assistance; and
(f) Systems shall be configured to disallow the reuse of the previous 24 Administrator
passwords.

Guidelines: Passwords may exceed 15 characters so long as agency business processes are not
negatively impacted (Note: the maximum password length for a Windows system is 127
characters).

**IA-14: PASSWORD REQUIREMENTS FOR SERVICE ACCOUNTS**
Service accounts are accounts that are used to facilitate automated processing. In general,
service accounts are not user-interactive since personnel are not able to log on to them.

(a) Passwords for service accounts are required to be at least fifteen (15) characters in length.
   Passwords may exceed 15 characters so long as agency business processes are not
   negatively impacted;
(b) Passwords will not contain the user’s account name or parts of the user’s full name that
    exceed two consecutive characters;
(c) Passwords are required to contain characters from each of the following four categories:
   (1) English uppercase characters (A through Z);
   (2) English lowercase characters (a through z);
   (3) Base 10 digits (0 through 9); and
   (4) Non-alphanumeric characters (for example: ! $ # > %);
(d) Service account passwords are required to be changed at least every 365 days or
    immediately upon the suspected compromise of the password;
(e) Systems shall be configured to prohibit service account passwords from being changed
    more than once in a 24-hour period. If it is necessary for a service account password to
    be changed more than once within a 24-hour period, the Agency’s IT Service Desk must
    be contacted for assistance; and
(f) Systems shall be configured to restrict service accounts from reusing their previous 24 passwords.

Guidelines: Passwords may exceed 15 characters so long as agency business processes are not negatively impacted (Note: the maximum password length for a Windows system is 127 characters).

**IA-15: PASSWORD REQUIREMENTS FOR PUBLICLY-FACING WEB APPLICATIONS**

Agencies shall protect public-facing web applications requiring authentication by deploying reasonably-expected security controls, including but not limited to the following requirements:

(a) Passwords having the following attributes:

(1) Required to be at least eight (8) characters in length;

(2) Not contain the user’s account name or parts of the user’s full name that exceed two consecutive characters;

(3) Required to contain characters from each of the following four (4) categories:
   a. English uppercase characters (A through Z);
   b. English lowercase characters (a through z);
   c. Base 10 digits (0 through 9); and
   d. Non-alphanumeric characters (for example: !, $, #, >, %);

(b) For publicly-accessible web applications that provide the general public with access to Sensitive Personally Identifiable Information (SPII), agencies shall offer users the option of using Multi-Factor Authentication for added protection, as technically feasible;

(c) For publicly-accessible web applications that provide agency personnel with access to agency systems containing sensitive information, multi-factor authentication shall be required;

(d) Default session timeout after a period of fifteen (15) minutes of inactivity; and

(e) Account lockout after five (5) failed login attempts.

Guidelines: Agency websites often provide the general public with access to SPII (e.g. pay stubs, retirement, and health benefits information, etc.) which if accessed without authorization could result in significant harm to individuals. The option to use multi-factor authentication to access an individual’s SPII information provides an added layer of protection for the individual. Additional security requirements for publicly-accessible applications and services can be found in the Security for Publicly Accessible Websites and Services Policy.
IA-16: RESTRICTIONS ON DISPLAYING PASSWORDS
Agency information systems that require passwords shall mask, suppress, or otherwise obscure the password upon entry to prevent unauthorized disclosure.

IA-17: SESSION LOCK
Agencies shall ensure systems are configured to prevent access to the system:

(a) After receiving a manual command from the user to implement a session lock; and
(b) Automatically implementing a session lock after fifteen (15) minutes of inactivity.

Guidelines: Session locks are temporary actions taken to prevent further access to an information system until the user re-authenticates to the system. Upon activation of a session lock the contents of the screen are hidden from view and access to the system is halted. Typically, screen savers are displayed upon the activation of a session lock.

IA-18: PKI-BASED AUTHENTICATION
Agencies shall ensure the agency information system for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
(b) Enforces authorized access to the corresponding private key;
(c) Maps the authenticated identity to the account of the individual or group; and
(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information using the network.

IA-19: PERIODIC REVIEW
Agencies shall document and implement a formal process to periodically review users’ access rights in order to maintain effective controls over user access to information assets. To maintain these effective controls, agencies are required to:

(a) Review user access to resources at least every six (6) months. The review should specifically identify and revoke access for, or remove the following:
   (1) Active User-IDs that are no longer needed;
   (2) User-IDs assigned to terminated users with active access;
   (3) Generic or anonymous User-IDs that are no longer needed;
   (4) Redundant or duplicate User-IDs;
   (5) User-IDs with excessive privileges, which are no longer necessary and/or are not approved; and
   (6) Maintain evidence that documents the reviews were completed;
(b) Establish procedures to monitor the events and activities of each user accessing agency systems, networks and information assets to detect deviations from authorized use; and

(c) Establish controls to ensure that logon activity is monitored and logged to a centralized log management system.

Guidelines: Agency CISOs should implement periodic review processes for account management as per their information security governance, risk, and compliance responsibilities.

REFERENCES
The requirements established in the Identity and Authentication Policy have been derived from the following:

- NIST SP 800-53 Access Controls (AC), Identity and Authentication (IA), Media Protection (MP);
- NIST CSF Protect/Access Controls (PR.AC); and
- NIST Special Publication (SP) 800-63-3: Digital Authentication Guidelines.
REMOTE ACCESS (RA)

PURPOSE
The purpose of the Remote Access Policy is to define accepted remote access practices and standards necessary to protect State of New Jersey networks, systems and services from unauthorized access and misuse.

KEY TERMS
Access - Ability to make use of an information asset.

CloudConnect - A bundled offering of cloud-based Microsoft Office365 products, including email, instant messaging, video conferencing, file sharing, and storage. It enables user-friendly interagency communication and file sharing, multi-device content synchronization, and two-factor authenticated remote access.

Direct Application Access Architecture – A high-level remote access architecture that allows users to access an individual application directly, without using remote access software (e.g. web-based access to CloudConnect web applications, Citrix Xenapp application virtualization service, etc.).

Multi-factor authentication – Authentication using two or more factors to achieve authentication. Factors include: something you know (e.g. password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g. biometric).

Multi-homed connection – A host connected to two or more networks or having two or more network addresses. For example, a computer may be connected to multiple Local Area Networks (LANs).

Network-Level Connection – The connection provides access to a State Agency’s private network through tunneling or a remote desktop access architecture and the software and data that reside on the internal information assets.

Remote Access - Access to a State of New Jersey information asset by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

Remote Desktop Access Architecture – A high-level remote access architecture that gives a user the ability to remotely control a particular computer at their agency from an external network. Remote desktop access architecture includes, but is not limited to, systems (local and remote) and software (e.g. Cisco AnyConnect, Citrix, GoToMyPC, Verisign Identity Protection (VIP)) that is used to facilitate and secure the remote session. The specific technologies utilized in a remote desktop access architecture are determined by the New Jersey Office of Information Technology.
**Split Tunneling** – The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network.

**Strong password** – A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

**Virtual Private Network (VPN)** – A virtual network, built on top of existing physical networks, that provides an encrypted communications tunnel for data and other information transmitted between networks.

**Web-Based Connection** – The connection provides access to one or more applications through a single centralized interface, through a direct application access or portal architecture, typically a web-browser to a portal server located within the demilitarized zone (DMZ). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network.

**RA-01: POLICY**

Agencies shall strictly control remote access to non-public State of New Jersey networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established.

This policy is supported by the following standards and guidelines.

**RA-02: CENTRALIZED MANAGEMENT OF REMOTE ACCESS INFRASTRUCTURE**

Unless otherwise authorized by the State Chief Technology Officer (CTO), the New Jersey Office of Information Technology (NJOIT) shall develop, implement, and manage enterprise remote access solutions and processes that provide authorized individuals within agencies of the Executive Branch of New Jersey State Government with remote access to agency-specific information resources.

The State CTO or his/her designee(s) is responsible for:

(a) Implementing and managing the State of New Jersey remote access infrastructure;

(b) Documenting approved technologies and methods of remote access to State of New Jersey information systems;

(c) Establishing usage restrictions and implementation guidance for each allowed remote access method;

(d) Monitoring for unauthorized remote access to information systems;
(e) Authorizing remote access to information systems prior to connection;

(f) Enforcing requirements for remote connections to information systems; and

(g) Immediately deactivating remote access to users, vendors, business partners, and other third-parties when it is no longer needed.

Guidelines: Consistent with Executive Order 225, the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual, the stated policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term “agency” includes NJOIT and all ancillary departments and agencies.

Remote access is access to State of New Jersey information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Virtual Private Networks (VPNs), when adequately provisioned with appropriate security controls, are considered internal networks.

All devices remotely logging into the internal network should be managed by the Agencies, with remote control of their configuration, installed software, and patch levels. Third-party devices (e.g., contractors/vendors) that are used for remote access to agency systems are required to be configured in accordance with the Endpoint Security Policy contained in this Manual. Agencies should consider controlling and managing configurations of remote access devices by implementing Network Access Control (NAC) solutions.

**RA-03: REMOTE ACCESS SECURITY**

The following general controls shall be implemented by NJOIT and agencies that provide users with remote access to information assets to ensure remote access is effectively controlled.

(a) Remote access to internal networks, systems, applications or services shall only be provided through technologies and methods authorized by the State Chief Technology Officer or his/her designee(s);

(b) All remote access sessions to agency internal networks shall be routed through NJOIT-managed network access control points;

(c) Where technically feasible, remote access sessions will be automatically monitored and controlled;

(d) Strong cryptography shall be implemented to protect the confidentiality and integrity of remote access sessions;

(e) All remote access sessions shall require the use of multi-factor authentication;
(f) Remote access connections to the internal networks shall be permitted only if the following criteria for the remote information system are met:

(1) Software patch status is current; and
(2) Anti-malware software is enabled and current;

(g) Where technically feasible, remote access solutions shall:

(1) Validate the patch level and software versions of mobile devices attempting to connect to the agency networks; and
(2) Prohibit the connection from granting access until the mobile device has the latest available security-related patches installed;

(h) All remote access infrastructure shall be configured to force an automatic disconnect of remote access sessions after a fifteen (15) minute period of inactivity;

(i) Asset custodians shall configure VPN technologies to limit VPN sessions to internal network assets to no greater than four (4) consecutive hours before a forced disconnect and the establishment of a new session is required;

(j) Agencies shall develop processes to limit the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs;

(k) Agencies shall develop processes to restrict remote network connections for vendors or other third-parties to only when required to perform a valid business function, and must be immediately deactivated after use;

(l) Where technically feasible, asset custodians shall configure any device in the session path to enforce, monitor, or log usage of all activities;

(m) Asset custodians shall audit and log remote access connections and associated activities; and

(n) Agencies shall forward all remote access logs to the NJCCIC enterprise Security Information and Event Management (SIEM) system in accordance with the Continuous Monitoring Policy as documented in this Manual.

Guidelines: The purpose of establishing maximum duration for VPN sessions is to ensure security of State information assets being accessed by users. The maximum duration requirement does not apply to extranet system-system remote access connections.

Automated monitoring and control of remote access sessions allow organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Limiting the number of access control points for remote accesses reduces the attack surface for organizations.
Allowing vendors to have 24/7 access to the network for support purposes increases the chances of unauthorized access, either from a user in the vendor's environment, or from a malicious individual who finds and uses this always-available external entry point into the network. Enabling access only for the time periods needed and disabling it as soon as it is no longer needed, helps prevent misuse of these connections.

**RA-04: AGENCY LEVEL AUTHORIZATION**
Before managers and/or supervisors authorize users to perform work via a remote access arrangement they must do the following:

(a) Identify the type of work to be performed through the remote access arrangement;

(b) Limit the authorization to only resources that are necessary to carry out the remote access arrangement safely and securely;

(c) Consider whether the needs to support the remote access arrangement can be met with less access and connectivity than provided at the main office; and

(d) As applicable, ensure a Remote Access Agreement between the remote access user and manager is signed and maintained in the agency file.

Guidelines: Work to be performed during an emergency situation to maintain essential operations may not warrant the remote access user to have the same access or connectivity as they do at their office.

**RA-05: TRAINING OF REMOTE ACCESS USERS**
Agencies shall ensure authorized remote access users receive security training, addressing at a minimum, the following subjects:

(a) The responsibilities outlined in this standard;

(b) The potential enterprise risks to both the Agency’s information assets and the information assets of other State agencies that are interconnected and/or available to authorized users through the Agency’s IT infrastructure;

(c) Protection of authenticators, such as passwords, personal identification numbers (PIN), and hardware tokens;

(d) Recognition of social engineering attack techniques and appropriate mitigation measures;

(e) The consequences for disabling, altering or circumventing the security configurations that protect State information assets; and

(f) Security incident management and breach disclosure procedures.

Guidelines: The remote access user training is to be provided in addition to the security training requirements as documented in the Security Awareness and Training Policy.
RA-06: REMOTE ACCESS USER RESPONSIBILITIES

Authorized remote access users shall be responsible for the following:

(a) Remote access users shall adhere to all applicable information security policies, standards, and procedures regarding the use of agency information assets, regardless of the work location;

(b) Remote access users shall ensure that all computing equipment that is connected to the State IT infrastructure network for remote access purposes has been configured in accordance with the Configuration Management and Endpoint Security policies documented herein;

(c) Remote access users shall not connect personally-owned information assets to the State IT infrastructure at the network-level;

(d) Remote access users shall only connect to State IT infrastructure through secure encrypted channels; and

(e) Remote access users shall ensure that information assets used to connect to the agency IT infrastructure are physically secured.

Guidelines: Just as in a user’s State office/facility, security measures cover not only information systems and technology, but all aspects of the information and information systems used by the user, including paper files, other media, storage devices, and telecommunications equipment (e.g., laptops, tablets, and smartphones) used to conduct their work duties. Remote users must keep all State property and information secure.

Remote access users are prohibited from disabling, altering, or circumventing established security controls on agency information assets used to connect to agency IT infrastructure, such as endpoint protection software (anti-virus/anti-malware), host-based firewalls, and content filtering software.

Encrypted channels may include encrypted virtual private networks (VPNs), encrypted web access, encrypted broadband, and encrypted dial-up connections. At no time may the remote access user initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).

REFERENCES

The requirements established in the Remote Access Policy have been derived from the following:

- NIST SP 800-53 System and Communication Protection (SC), Access Control (AC);
- NIST CSF Protect/Access Controls (PR.AC); and
SECURITY ENGINEERING AND ARCHITECTURE (SE)

PURPOSE
The purpose of the Security Engineering and Architecture policy is to align information security decisions with the enterprise information technology architectural strategy and industry-recognized leading practices for secure engineering.

KEY TERMS
System Development Life Cycle (SDLC) - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

SE-01: POLICY
Agencies shall ensure that security engineering and architecture principles are implemented in all information assets, such that they incorporate industry recognized leading security practices and address all applicable statutory, regulatory, and contractual obligations.

This policy is supported by the following standards and guidelines.

SE-02: SECURITY ENGINEERING PRINCIPLES
Asset owners and asset custodians are required to:

(a) Implement configuration standards for all system components that are consistent with industry-accepted system hardening standards and address known security vulnerabilities; and

(b) Maintain appropriate documentation related to system component configuration including reasons why certain standards cannot be implemented.

Guidelines: Agencies are to apply security engineering principles primarily to new development systems or systems undergoing major upgrades. For legacy systems, security engineering principles must be applied to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example:

- Developing layered protections to employ Defense-in-Depth;
- Establishing and documenting sound security policy, architecture, and controls as the foundation for design;
- Incorporating security requirements into the system throughout its life cycle;
- Delineating physical and logical security boundaries;
- Ensuring system developers are trained on how to build secure software;
• Tailoring security controls to meet agency and operational needs;
• Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
• Reducing risk to acceptable and documented levels, thus enabling informed risk management decisions.

Agencies shall adhere to industry-accepted system hardening standards. Acceptable hardening standards include, but are not limited to, those from the following resources:

• Center for Internet Security (CIS) Security Benchmarks;
• National Institute of Standards Technology (NIST);
• Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); and/or
• Vendor-specific hardening directions.

The CIS Security Benchmarks are consensus-based, best-practice security hardening standards and configuration guides that have been both developed, and accepted by, government, business, industry, and academia. The NJCCIC maintains a state-wide subscription to the CIS Security Benchmarks and Configuration Assessment tools. Agencies should contact the NJCCIC to gain access to CIS Security Benchmarks portal.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160, *Systems Security Engineering*, is the default guide for security related to engineering trustworthy, secure systems.

**SE-03: ALIGNMENT WITH ENTERPRISE ARCHITECTURE**

The State Chief Technology Officer and his/her designees in the NJ Office of Information Technology shall develop an enterprise architecture that is:

(a) Aligned with the industry-recognized leading practices;
(b) Utilized in all system development and acquisition activities; and
(c) Inclusive of security architecture requirements.

Guidelines: The information security architecture at the individual system level is to be consistent with, and complement, the more global, enterprise-wide information security architecture that is integral to, and developed as, part of the State enterprise architecture.

The integration of information security requirements and associated security controls into the State enterprise architecture, as defined by NJOIT, helps to ensure that security considerations are addressed early in the System Development Life Cycle (SDLC) and are directly and explicitly related to the State’s and the respective agency’s mission and business processes. This also embeds into, and links with, the State enterprise architecture, and integral information security architectures consistent with risk management and information security strategies.
In support of industry-recognized leading practices:

- Implementation of vendors’ industry-recognized security leading practices should be used when configuring a vendor’s product, unless there is a valid, documented and appropriately reviewed business or security requirement to deviate from the recommended industry-recognized leading practices in deploying and operating those solutions; and

- If a best practice cannot be implemented, compensating controls should be employed and documented accordingly.

**SE-04: SECURE CONFIGURATIONS**

Agency asset custodians are required to develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production systems hardening includes, but is not limited to:

(a) Verifying that system configuration standards are:

   (1) Updated as new vulnerability issues are identified;
   (2) Applied when new systems are configured;
   (3) Consistent with industry-accepted hardening standards;

(b) Where feasible, implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers and database servers should be implemented on separate servers);

(c) Enforcing least functionality, which includes but is not limited to:

   (1) Allowing only necessary services, protocols, and daemons;
   (2) Removing all unnecessary functionality, which includes but is not limited to:

      i. Scripts;
      ii. Drivers;
      iii. Features;
      iv. Subsystems;
      v. File systems; and
      vi. Services (e.g. web, mail, FTP, RDP);

(d) Implementing security features for any required services, protocols or daemons that are considered to be insecure, which include but, are not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP;

(e) Verifying system security parameters are configured to prevent misuse; and
Documenting the functionality present on information systems.

Guidelines: For baseline configurations, agencies shall adhere to industry-accepted system hardening standards. Acceptable hardening standards include but are not limited to those from the following resources:

- Center for Internet Security (CIS) Security Benchmarks;
- National Institute of Standards Technology (NIST);
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); and/or
- Vendor-specific hardening directions.

The implementation of industry-recognized security leading practices should be used when configuring a vendor’s product, unless there is a valid business or security requirement to deviate from the recommended industry-recognized leading practices in deploying and operating those solutions. If a best practice cannot be implemented, compensating controls should be employed and documented accordingly.

If virtualization technologies are used, verify that only one primary function, where technically feasible, is implemented per virtual system component or device.

**SE-05: LEAST PRIVILEGE**

Asset custodian shall employ the principle of least privilege, which states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary. Asset custodians are required to:

(a) Identify and remove insecure services, protocols, and ports;

(b) Enable only necessary and secure services, protocols, and daemons, as required for the function of the system;

(c) Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);

(d) Verify services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings; and

(e) Remove all unnecessary functionality, such as:

1. Scripts;
2. Drivers;
3. Features;
4. Subsystems;
5. File systems; and
6. Services (e.g. web, mail, FTP, remote control and administration).
Guidelines: Asset custodians should review functions and services of information systems, to determine which functions and services are candidates for elimination (e.g., Instant Messaging, auto-execute, and file sharing). Agencies may utilize network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

**SE-06: SECURITY FUNCTION ISOLATION**
Agency asset custodians and asset owners are required to implement isolation techniques to prevent functions that require different security levels from co-existing on the same server. Isolation techniques include, but are not limited to:

(a) Where feasible, implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server;

(b) Configure firewall and router configurations to restrict connections between untrusted networks and any system components in a trusted, internal network;

(c) Demilitarized Zones (DMZs) need to be implemented to limit inbound traffic to only system components that provide authorized and publicly accessible services, protocols, and ports;

(d) Servers that access external networks or are accessed from external networks need to be logically isolated from the internal networks;

(e) Networks need to be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices;

(f) Switched network technology needs to be utilized, when possible, to prevent eavesdropping, session-stealing or other exploits based on the accessibility of network traffic; and

(g) Information resources with higher protection requirements for confidentiality should not have a trusted relationship with a system that has lower protection requirements.

Guidelines: Where feasible, system security functions should be isolated from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to, and protects the integrity of, the hardware, software, and firmware that perform those security functions. An “untrusted network” is any network that is external to the networks belonging to the agency, and/or which is out of the agency’s ability to control or manage. Systems must restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

**SE-07: DEFENSE IN-DEPTH**
Agencies shall employ a Defense-in-Depth (DiD) architecture to protect the confidentiality, integrity, and availability of systems and information, placing systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.
Guidelines: The implementation of layered defenses with minimized interactions among security functions and independent layers (e.g., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

**SE-08: APPLICATION PARTITIONING**
Where technically feasible, asset custodians and data/process owners are required to configure systems such that user functionality (including user interface services) is separated from information system management functionality. Separation may be accomplished through the use of one or more of the following:

(a) Network segmentation;
(b) Different computers;
(c) Different instances of the operating system;
(d) Different network addresses; or
(e) Other methods as appropriate.

Guidelines: An example of this separation is where user interface services (e.g., public web pages) are implemented separately from storage and management services (e.g., administrative or database management). Agencies can implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate.

**SE-09: SYSTEM PARTITIONING**
Where technically feasible, asset custodians are required to partition critical systems to reside in separate physical domains or environments:

(a) Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations, but based on higher risk should not be installed within a networked environment; and
(b) Critical services should operate on separate, physical or logical host machines, such as DNS, file, mail, web, and database servers.

Guidelines: System partitioning is part of a defense-in-depth protection strategy. Agencies are to determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.
**SE-10: FIREWALL AND ROUTER CONFIGURATIONS**

Asset custodians are required to establish firewall and router configuration standards that include the following:

(a) Asset custodians are required to establish and maintain a formal process for approving and testing all network connections and changes to both firewall and router configurations;

(b) Asset custodians are required to establish and maintain detailed network diagrams. Network diagrams must:
   
   1. Document all connections including any wireless networks;
   2. Be reviewed annually; and
   3. Be updated as the network changes to reflect the current architecture in place;

(c) Asset custodians are required to establish and maintain detailed data flow diagrams that show data flows across systems and networks;

(d) A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and agency(s) internal networks;

(e) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes;

(f) A documented business justification is required for all services, protocols, and ports allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure; and

(g) Firewall and router rule sets must be reviewed at least once every six (6) months and cover the following:
   
   1. Validation of Access Control Lists (ACLs); and
   2. Vulnerability management (e.g., validating software and firmware is current).

Guidelines: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP);
- Hypertext Transfer Protocol (HTTP); and
- Telnet.

**SE-11: SECURE LOG-ON**

Information systems establish a trusted communications path between the user and the security functions of the system. Where technically feasible, information systems must authenticate with Active Directory (AD).

Guidelines: A trusted path is simply some mechanism that provides confidence that the user is communicating with what the user intended to communicate with, ensuring that attackers can't
intercept or modify whatever information is being communicated. The traditional example is a "fake login" program (e.g., a program is written to look like the login screen of a system) where when users try to log in, the fake login program can then capture user passwords for later use.

Microsoft’s Active Directory provides a trusted path to its login window by requiring the user to press Ctrl+Alt+Del. This key sequence causes a non-maskable interrupt that can only be intercepted by the operating system, thus providing reasonable assurances that the login window cannot be spoofed by any application.

**SE-12: PREVIOUS LOGON NOTIFICATION**

Where the capability exists, asset custodians are required to configure the information system to notify the user, upon successful logon/access, previous logon information. This previous logon information is to include the date and time of the last logon; the location of the logon; and the number of unsuccessful logon attempts since the last successful logon. The user must perform some action to remove the notice.

Guidelines: This control provides the user with notice of previous logons and may allow for detection of unauthorized access to a user’s account.

**SE-13: LOGON BANNER**

Where technically feasible, asset custodians are to configure State information systems to display an agency-defined notification banner that is displayed to users before granting access to the system. The notification banner shall include privacy and security notices consistent with applicable Federal and State laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall:

(a) State the following:

   (1) Users are accessing an information system owned and/or operated by the State of New Jersey;

   (2) Information system usage may be monitored, recorded, and subject to audit;

   (3) Unauthorized use of the State information system is prohibited and subject to criminal and civil penalties; and

   (4) Use of the State information system indicates consents to monitoring and recording of all user actions and interactions.

(b) Retain the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to, or further access the State information system.

Guidelines: An example of a logon banner that may be used includes the following:

This is a State of New Jersey information system which may be accessed and used only for official government business by authorized personnel. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative action. Administrative action may include
discipline, up to and including, termination of employment or contract. All information on this system may be intercepted, recorded, read, copied, or disclosed by, and to, authorized personnel for official purposes, including, criminal, civil and/or administrative investigations. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.

SE-14: FAIL SECURE IN KNOWN STATE
Where technically feasible, agency asset custodians and data/process owners are required to configure assets to fail in a known state, or safe mode, in order to preserve system state information at the time of the failure.

Guidelines: This is used to manage risk to specialized systems (e.g. firewalls), including operational technology (e.g., ICS, SCADA, DCS, and PLC) consistent with risk analysis.

Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, and application gateways residing in the demilitarized zone or other protected subnetworks), information systems do not enter insecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

SE-15: FAIL-SAFE PROCEDURES
Asset custodians and data/process owners are required to configure critical systems to implement fail-safe procedures when failure conditions occur.

Guidelines: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take.

SE-16: CLOCK SYNCHRONIZATION
Network Time Protocol (NTP) is the State’s official method of synchronizing all system clocks and times. Agencies shall ensure that:

(a) Asset custodians configure agency NTP servers so that they are receiving time from NJOIT approved time sources; and

(b) Data/process owners ensure NTP on their systems is configured properly and validate the following:

(1) Systems are configured to synchronize time with NJOIT’s or NJOIT-approved NTP servers;

(2) Information systems have the correct and consistent time; and

(3) Time data is protected from unauthorized modification.
Guidelines: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO. To ensure time is synchronized across all systems on the GSN agencies should use NJOIT’s time servers.

REFERENCES
The requirements established in the Security Engineering and Architecture policy have been derived from the following references:

- NIST SP 800-53: Planning (PL), Project Management (PM), Systems and Services Acquisition (SA), Security Assessment and Authorization (CA), System and Information Integrity (SI); System and Communication Protection (SC);
- NIST CSF: Protect – Protective Technology (PR-PT); and
PURPOSE
The purpose of the Configuration Management Policy is to ensure that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of all State information assets.

KEY TERMS
System Development Life Cycle (SDLC) - The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

CM-01: POLICY
Agencies shall implement a configuration management program that establishes and maintains the secure configuration of the system throughout its life cycle.

This policy is supported by the following standards and guidelines.

CM-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS
Baseline security requirements that comply with applicable legal, statutory, and regulatory compliance obligations shall be established for all agency owned or managed assets:

(a) Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template;

(b) Deviations from standard baseline configurations must be authorized following change management processes prior to deployment, provisioning, or use; and

(c) Unless a technical or business reason exists, standardized images shall be used to represent hardened versions of the underlying operating system and the applications installed on the system. These images must be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

(d) Naming conventions for devices located on agency networks should give no indication of the purpose or the owner of the device.

Guideline: Technology platforms includes but are not limited to:

- Firewalls;
- Routers;
- Switches, capable of being managed;
Wireless Access Points (WAPs);
Servers;
Workstations;
Embedded devices; and
Mobile Devices, capable of being managed.

Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Center for Internet Security (CIS);
- Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs);
- Microsoft Security Configuration Wizard; and
- Other vendor provided secure configuration settings.

The NJCCIC maintains a state-wide subscription for Center for Internet Security benchmarks. Agencies wishing to obtain access to CIS benchmarks and configuration assessment tools may contact the NJCCIC at security@cyber.nj.gov.

Agencies must consider that attackers will seek out high-value targets when deciding which systems to target. High value targets include such systems as domain controllers, sensitive data repositories, and others. Including “DC” or “Cardholder Data” or other such descriptors in the system’s name is not permitted. Similarly, including the device owner’s name or User-ID (e.g. “<User-ID>-PC” or “<User-ID>-Laptop”) within the name of the device is highly discouraged.

**CM-03: AUTOMATED CENTRAL MANAGEMENT AND VERIFICATION OF BASELINE CONFIGURATIONS**

Where technically feasible, agencies shall employ automated mechanisms to verify standard device configurations and detect changes. This includes but is not limited to:

(a) Implementing and testing an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts asset custodians and security personnel when unauthorized changes occur;

(b) Logging all alterations to such files and automatically reporting deviations to security personnel;

(c) Detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system; and

(d) Devising a list of authorized software and version that is required for each technology platform, including servers, workstations, and laptops of various kinds and uses.
Guidelines: Whenever possible agencies should use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration. Automated mechanisms that help agencies maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels.

The NJCCIC maintains enterprise licenses for automated configuration assessment tools. Agencies wishing to obtain access to licensed configuration assessment tools may contact the NJCCIC at security@cyber.nj.gov.

**CM-04: LEAST FUNCTIONALITY**

Agencies shall adhere to the “principle of least functionality” when configuring systems to provide only essential capabilities and specifically prohibit or restrict the use of the following functions, ports, protocols, and/or services. Agencies shall:

(a) Identify and remove insecure services, protocols, and ports;

(b) Enable only necessary and secure services, protocols, and daemons, as required for the function of the system;

(c) Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);

(d) Verify services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings; and

(e) Remove all unnecessary functionality, such as:

(1) Scripts;

(2) Drivers;

(3) Features;

(4) Subsystems;

(5) File systems; and

(6) Unnecessary web services.

Guidelines: Agencies should review functions and services of systems, to determine which functions and services are candidates for elimination (e.g., Instant Messaging, SMS, auto-execute, and file sharing). Agencies may employ network intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
CM-05: SOFTWARE USAGE RESTRICTIONS

Agencies are required to implement controls to ensure users utilize software in accordance with license agreements and copyright laws.

Guidelines: Agencies should implement a software inventory system that tracks the version of the underlying operating system as well as the applications installed on it. The software inventory system should be correlated to the hardware asset inventory, so all devices and associated software are tracked from a single location. Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on agency needs.

REFERENCES

The requirements established in the Configuration Management policy have been derived from following:

- NIST SP 800-53 Configuration Management (CM), System and Information Integrity (SI); and
- NIST CSF Protect/Information Protection Policies and Procedures (ID.PR).
ENDPOINT SECURITY (ES)

PURPOSE
The purpose of the Endpoint Security policy is to ensure that endpoint devices are properly configured, and measures are implemented to protect State information and information systems from a loss of confidentiality, integrity, and availability. This policy establishes the criteria that endpoint devices must meet prior to being granted access to agency networks.

KEY TERMS
**Endpoint** - Any device capable of being connected, either physically or wirelessly to a network and accepts communications back and forth across the network. Endpoints include, but are not limited to: computers, servers, tablets, mobile devices, or any similar network enabled device.

**Least Privilege** - The principle of least privilege states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary. The principle of least privilege is also commonly referred to as the principle of least functionality.

**ES-01: POLICY**
Agencies shall implement the concept of “least functionality” for all endpoints and proactively govern security mechanisms to keep their technology assets secure from evolving threats.

This policy is supported by the following standards and guidelines.

**ES-02: INVENTORY OF ENDPOINT DEVICES**
Any endpoint that processes, transmits and/or stores State data must be inventoried and configured in accordance with the protection requirements necessary to protect the asset from a loss of confidentiality, integrity, and/or availability.

**ES-03: SECURITY CATEGORIZATION OF ENDPOINT**
Endpoints shall inherit the highest security categorization of the information it generates, stores, processes, or transmits and will be protected with security controls commensurate with risk and potential impact should there be a loss of confidentiality, integrity, and/or availability.

Guidelines: If an endpoint that stores or processes various types of information, such that some is categorized as High Impact, while other information is categorized as Moderate or Low Impact, then the endpoint shall be categorized as High Impact and all the controls required for a High-Impact asset must be implemented.
**ES-04: SOFTWARE CURRENCY**

Agencies shall implement procedures to ensure all endpoints including their operating systems, application software, and components, maintain software currency throughout the endpoint’s lifecycle such that:

(a) All operating system and application software are protected from known vulnerabilities by having the latest applicable vendor-supplied security patches installed;

(b) Critical security patches are installed as soon as practical but no later than thirty (30) days after the vendor’s release date; and

(c) Non-critical security patches are installed as soon as practical, but no later than ninety (90) days after the vendor’s release date.

Guidelines: Agencies are advised to apply a risk-based approach to prioritize its patch installations.

**ES-05: ACCESS CONTROLS**

Physical and logical access controls must be implemented to ensure endpoint protection. All endpoints shall be configured with access controls as required in the Access Management Policy. Agencies must establish access controls in accordance with the requirements described below.

(a) **Least Privilege** - Access should be limited to only those authorized users necessary to accomplish the assigned tasks in accordance with the agency’s mission and business functions;

(b) **Privilege Levels** - Establish non-privileged and privileged levels of users; and

(c) **Privileged Access** - Prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards and countermeasures.

**ES-06: SESSION LOCK**

As technically and operationally feasible, agencies are required to implement automated session lock controls to disable access to an endpoint after an established period of inactivity.

(a) For tablets, smartphones, and wearable devices, the session lock shall be configured to no more than 5 minutes of inactivity; and

(b) For all other endpoints (e.g. desktops, laptops, servers) the session lock shall be configured to no more than 15 minutes of inactivity.

**ES-07: DATA PROTECTION MEASURES**

As technically feasible, agencies shall protect sensitive information by employing cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest.

Guidelines: This addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when
it is located on storage devices as specific components of systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Agencies may employ different mechanisms to achieve confidentiality and integrity protections. Agencies may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved.

ES-08: PROTECTION AGAINST MALICIOUS CODE
As technically feasible, agencies shall deploy anti-malware software on all endpoints capable of running anti-malware software, including, but not limited to laptops, desktops, servers, tablets, and smartphones.

(a) Anti-malware software must be configured to perform periodic scans of the endpoint and real-time scans of all files from external sources as the files are downloaded, opened, or executed;

(b) Anti-malware software must be configured to quarantine any malicious code detected, and to send an alert to the agency’s IT service desk and/or information security team;

(c) Anti-malware software must be configured to automatically apply and keep current with anti-malware vendor updates;

(d) Asset custodians are responsible for ensuring that anti-malware mechanisms are actively running and cannot be disabled or altered by users; and

(e) Anti-malware software shall be configured to maintain an audit log of all anti-malware software activity

Guidelines: The term malware refers to any malicious code including viruses, logic-bombs, ransomware, etc. Endpoints not capable of running anti-malware software should have a documented business justification as to why anti-malware software cannot be implemented and the compensating controls that are in place to minimize the risk associated with the lack of anti-malware software on that endpoint.

ES-09: FILE INTEGRITY MONITORING (FIM)
As technically feasible, asset custodians who manage endpoints that are deemed critical shall:

(a) Deploy File Integrity Monitoring (FIM) tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly;

(b) Verify the use of FIM tools by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:

(1) System executables;
(2) Application executables;
(3) Configuration and parameter files; and
(4) Centrally stored, historical or archived, log and audit files; and
(c) Verify the tools are configured to alert personnel to unauthorized modification of critical files and to perform critical file comparisons.

Guidelines: FIM tools should be used to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a User-ID switch, such as with the su or sudo command).

These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

**ES-10: HOST-BASED FIREWALL**

As technically feasible, agencies are required to install and maintain host-based firewalls on endpoints that directly access the Internet, including but not limited to mobile devices such as laptops, tablets, and smartphones. The host-based firewall shall be configured to:

(a) Default-deny (drop) all traffic except those services and ports that are explicitly permitted by the agency; and

(b) The configuration settings of the software must not be alterable by standard users.

Guidelines: A host-based firewall is a software application that controls network traffic to and from the endpoint on which it is installed, unlike a network firewall that controls traffic between two or more networks. Host-based firewalls allow a security policy to be defined for individual computers, whereas a network firewall controls the policy between the networks that it connects. Many current operating systems, including Microsoft Windows, include host-based or “personal” firewalls as part of the operating system. Third-party host-based firewalls are also included as features for various vendors’ endpoint protection software offerings. Agencies should determine the best host-based firewall solution for their respective business and security needs and implement it on all Internet-accessible endpoints they manage. Additional guidance on endpoint security software solutions can be obtained from the Office of Homeland Security, Division of Cybersecurity.

**ES-11: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS/HIPS)**

Where technically feasible, asset custodians are required to install host-based intrusion detection and prevention system (HIDS/HIPS) software or similar security technologies on endpoints (i.e. servers) that store, process, generate or transmit sensitive information, or where the endpoint is
deemed critical to an agency’s business functions. HIDS/HIPS alerts are to be sent to the agency’s Security Incident Event Management (SIEM) or centralized log collector. If an agency does not have a SIEM or centralized log collector then the alerts are to be forwarded to the NJCCIC enterprise Security Incident Event Management (SIEM).

Guidelines: HIDS/HIPS software monitors a single endpoint for suspicious activity by analyzing events occurring within that endpoint, whereas a network intrusion detection and prevention system monitors traffic on a network. Some endpoint protection packages include HIDS/HIPS technologies as part of an overall security suite (e.g. anti-virus, anti-malware, firewall, HIDS/HIPS). In consultation with the OHSP Division of Cybersecurity, agencies should determine the best endpoint and HIDS/HIPS solution for their respective business and security needs.

**ES-12: MOBILE CODE SECURITY**

Agencies must implement procedures to manage the use of mobile code technologies (i.e. Java, ActiveX, Flash, etc.) on endpoint devices that operate independent of the device’s operating system.

(a) Define acceptable and unacceptable mobile code and mobile code technologies (e.g., Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript);

(b) Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

(c) Authorize, monitor, and control the use of mobile code within the agency information system.

Guidelines: Operating system independent applications promote functionality across platforms but are considered security risks. Decisions regarding the employment of mobile code within agency systems should be based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and mobile devices. Agencies should strongly consider prohibiting the installation of mobile code technologies that would allow unmediated access to system services and resources.

**ES-13: TRUSTED PATH**

As technically feasible, and to ensure systems establish a trusted communications path between the user and the system’s security function, all agency systems should authenticate with Active Directory (AD).

Guidelines: A trusted path is simply some mechanism that provides confidence that the user is communicating with what the user intended to communicate with, ensuring that attackers can’t intercept or modify whatever information is being communicated. The traditional example is a
"fake login" program (e.g., a program is written to look like the login screen of a system) when users try to log in, the fake login program can then capture user passwords for later use.

Microsoft’s Active Directory provides a trusted path to its login window by requiring the user to press Ctrl+Alt+Del. This key sequence causes a non-maskable interrupt that can only be intercepted by the operating system, thus guaranteeing that the login window cannot be spoofed by any application.

**ES-14: HYPERVISOR ACCESS**

On endpoints (e.g. servers and workstations) that host virtualized systems, agencies are required to implement controls that restrict access to all hypervisor management functions and/or administrative consoles based on the principle of least privilege. The access restrictions shall be supported by appropriate technical controls (e.g., multifactor authentication, audit logs, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).

**ES-15: PORT AND I/O DEVICE ACCESS**

As technically feasible, and in instances in which strong business and/or security risks exist, agencies shall disable connection ports or input/output devices on sensitive systems or system components.

Guidelines: Disabling or removing connection ports and I/O devices helps prevent exfiltration of information from systems and the introduction of malicious code into systems from those ports/devices. Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD), Digital Video Disk (DVD), and USB drives.

**ES-16: AUDIT LOGGING**

As technically feasible, audit logging must be implemented on all endpoints. Endpoints are to log the following information for each security event:

(a) User account, system account, service or process responsible for initiating the system event;

(b) Type of event;

(c) Date and time of event;

(d) Success or failure indication;

(e) Origination of event;

(f) Identity or name of affected data, system component, or resource;

(g) All successful login and logoff attempts;

(h) All unsuccessful login and authorization attempts;
(i) All identification and authentication attempts;

(j) All actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users);

(k) All actions, connections and requests performed by privileged functions;

(l) All changes to logical access control authorities (e.g., rights, permissions);

(m) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;

(n) The creation, modification and deletion of objects including files, directories and user accounts;

(o) The creation, modification and deletion of user accounts and group accounts;

(p) The creation, modification and deletion of user account and group account privileges;

(q) System start-up and shutdown functions;

(r) Modifications to administrator account(s) and administrator group account(s) including:
   
   (1) Escalation of user account privileges commensurate with administrator-equivalent account(s); and

   (2) Adding or deleting users from the administrator group account(s);

(s) The enabling or disabling of audit report generation services; and

(t) Command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Guidelines: Endpoints should record logs in a standardized format. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

REFERENCES
The requirements established in the Endpoint Security policy have been derived from the following:

• NIST SP 800-53 Media Protection (MP), System and Communications Protection (SC), Configuration Management (CM), System and Information Integrity (SI); and

• NIST CSF Protect – Data Security (PR.DS), Detect – Security Continuous Monitoring (DE.CM).
EMBEDDED SYSTEMS (EM)

PURPOSE
The purpose of the Embedded Systems Policy is to ensure risks, including risks to human safety, are accounted for and managed in the use of embedded technologies in State of New Jersey agencies, systems, and business processes.

KEY TERMS
Automation Technology – is the use of technology by which a process or procedure is performed without human assistance.

Embedded System - Specialized hardware and software that is wholly incorporated as part of a larger system or machine.

Industrial Control System - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Internet of Medical Things (IoMT) - is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks.

Internet of Things (IoT) - is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data.

Operational Technology (OT) - Operational Technology is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. The term has become established to demonstrate the technological and functional differences between traditional Information Technology systems and Industrial Control Systems.

Programmable Logic Controller (PLC) - or programmable controller is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

Supervisory Control and Data Acquisition (SCADA) - is a control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.
**Wearable Technology** - are smart electronic devices (electronic devices with micro-controllers) that can be worn on the body as implants or accessories.

**EM-01: POLICY**
In addition to ensuring confidentiality, integrity, availability, and privacy, agencies shall address safety with embedded technologies in an effort to prevent or mitigate risks to State of New Jersey personnel and the general public.

This policy is supported by the following standards and guidelines.

**EM-02: EMBEDDED TECHNOLOGY SECURITY**
Prior to implementing embedded technologies, agencies shall:

(a) Assess the safety-related risks associated with embedded technologies;
(b) Remediate vulnerabilities within embedded technologies; and
(c) Apply compensating controls where vulnerabilities cannot be remediated.

Guidelines: Embedded systems/technologies include, but are not limited to:
- Internet of Things (IoT) devices such as cameras; and/or
- Operational Technology (OT).

Examples of embedded systems include: digital cameras, GPS devices, vehicle embedded systems such as anti-locking brakes, home and office security systems, “smart devices” including phones, tablets and appliances, traffic monitoring devices, traffic lights, medical equipment, radiological and poisonous gas monitoring systems, etc. The use of embedded technologies will continue to grow in both home and business environments.

Agencies must consider data sensitivity and privacy, system criticality, and safety throughout the lifecycle of embedded technologies. Agencies must also consider the intended purpose and the environment where embedded technologies are used in order to account for associated risks. Prior to acquisition, agencies must consider the design of embedded technologies to ensure security controls, as well as the ability to patch vulnerabilities, is part of the design. Agencies are to implement a defense-in-depth strategy to limit any adverse impacts should a security layer be breached. The use of Network Access Control (NAC) solutions should also be considered to ensure embedded technology systems/devices connected to agency networks are accounted for and appropriately managed.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-183, *Network of Things*, is the default guide for security related to embedded technology.
**EM-03: INTERNET OF THINGS (IoT)**  
Agencies shall implement industry-recognized leading practices for the development, configuration, and maintenance of Internet of Things (IoT). IoT includes, but is not limited to:

(a) Wearable technology;
(b) Medical technology;
(c) Automation technology.

Guidelines: Leading practices for IoT are currently outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-183, *Network of Things*.

**EM-04: OPERATIONAL TECHNOLOGY (OT)**  
Agencies shall implement industry-recognized leading practices for the development, configuration, and maintenance of Operational Technology (OT). OT includes, but is not limited to:

(a) Industrial Automation and Control Systems (IACS);
(b) Supervisory Control and Data Acquisition (SCADA);
(c) Programmable Logic Controllers (PLC);
(d) Discrete Process Control Systems (DPC);
(e) Distributed Control Systems (DCS); and
(f) Industrial Control Systems (ICS).

Guidelines: Operational Technology is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. Leading practices for IACS and OT are currently outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82, *Guide to Industrial Control Systems (ICS) Security*.

**REFERENCES**  
The requirements established in the Embedded Technology Security Policy have been derived from the following:

- NIST Special Publication (SP) 800-183, *Networks of Things*;
- NIST Special Publication (SP) 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*;
- Groupe Spéciale Mobile Association (GSMA), *IoT Security Guidelines*; and
MOBILE DEVICE MANAGEMENT (MD)

PURPOSE
The purpose of the Mobile Device Management Policy is to establish the administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for State business purposes.

KEY TERMS
Bring Your Own Device (BYOD) – Refers to the policy of permitting employees and contractors to use personally owned or third-party owned mobile devices (e.g. tablets, and smart phones) for State business purposes.

Laptop Computer – A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. Unlike a mobile device, a laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities.

Mobile Application Management (MAM) – Mobile application management (MAM) and mobile application store (MAS) management perform application monitoring, reporting, security, and deployment.

Mobile Device – For the purposes of this Policy, a mobile device is defined as any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.

Mobile Device Management (MDM) – Is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints.

Nonpublic information – Is information that an employee obtains, or is provided access to, during his/her employment with the State of New Jersey that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:

(a) Is designated by the State or the Agency for which the employee works as nonpublic information;

(b) Contains markings such as “Confidential”, “Internal”, “Restricted”, or similar language, or is considered sensitive information;

(c) Contains information that must be protected by State or Federal Statute, State or Agency policy, or other regulation;

(d) Is provided to the State or the Agency for which the employee works by customers or third parties under agreement and with the understanding that it will be treated as
confidential, nonpublic information; or

(e) Contains information related to the internal State or Agency capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls.

**Sensitive information** – Is a term to describe any information which requires protection from unauthorized access or disclosure.

**Smartphone** – A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications.

**Tablet** – An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications and they are larger.

**Portable Storage Device** – An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

**MD-01: POLICY**

Agencies employing mobile computing devices for State business purposes shall implement processes and security controls commensurate with the information security risks introduced by the use of mobile devices.

This policy is supported by the following standards and guidelines.

**MD-02: AUTHORIZATION FOR USE OF MOBILE DEVICES**

The use of mobile devices for State business purposes is at the discretion of each agency. Participating agencies shall review and authorize the use of mobile devices for State business purposes consistent with their internal policies, procedures, applicable State and Federal laws and regulations, and the policies and standards contained in this Manual.

(a) Business Requirement: Mobile devices are provided for official State business use and may be made available or authorized for employees in positions where the associated benefits justify the additional operating costs and/or risks; and

(b) Discretionary Approval: Approval for either providing a user with a State-owned mobile device or allowing the use of a personally owned device for State business purposes, is at the discretion of each agency and the user’s manager/supervisor.
MD-03: RISK ASSESSMENT
Prior to deploying or authorizing the use of mobile devices for State business purposes, agencies must consider the risks associated with the use of mobile devices and establish processes and controls to mitigate them to acceptable levels.

Guidelines: As with all information assets, the ability to maintain the confidentiality, integrity, availability, and privacy of agency information should be the primary security objective. Agencies should consider the following threats when considering the risks associated with the use of mobile devices to conduct agency business.

Some of the threats introduced by mobile devices include:

- Theft/loss of device;
- Untrusted/Unsecure wireless networks;
- Phishing (email), Vishing (voice), Smishing (SMS/MMS);
- Rogue apps and malware:
  1. Mobile pick-pocketing: rogue apps may access mobile device resources and carry out fraudulent activities such as the generation of premium SMSs and premium phone-calls without user intervention or approval;
  2. Stealing of personal information: theft of information like contacts, SMSs and media files is widespread, especially on open platforms. A huge market exists for such databases;
  3. Spyware: Smartphones have features like cameras, microphones and GPS tracking. Several apps allow these features to be activated remotely without the user’s knowledge;
- Identity theft - This involves spoofing a phone’s parameters and details. Phones can then be used as a factor for authentication;
- Mobile botnets / relays - Smartphones with powerful 3G/4G connections can be used as nodes and relays in a botnet. These can be used to generate spam or launch Distributed Denial of Service (DDoS) attacks;
- Espionage - Leakage of sensitive information stored on mobile devices; and
- Access to app data and app user data: attention needs to be given to how applications use and store data.

MD-04: BRING YOUR OWN DEVICE (BYOD)
Agencies may opt to implement programs that allow employees and contractors to use personally owned or third-party owned mobile devices for State business purposes. Such arrangements are commonly referred to as Bring Your Own Device (BYOD). Personally owned
and third-party owned mobile devices present additional risks to agencies that offer BYOD arrangements.

(a) Agencies shall establish and implement a BYOD end-user agreement that clearly states the requirements that shall be met for a personally owned or third-party owned device to be used for State business purposes;

(b) Personally owned and third-party owned mobile devices are subject to the same security requirements as State-owned mobile devices set forth herein, as well as any additional policies or standards as dictated by the authorizing agency;

(c) Agencies offering a BYOD arrangement shall clearly state the security and support services that users of permitted personally owned mobile devices can expect. These security services may include mobile device management, password management, and remote wiping in case of loss, theft, device failure, upgrade, or change of ownership;

(d) The BYOD policy shall clarify the systems and services allowed for use or access on a BYOD-enabled device;

(e) Agencies offering a BYOD arrangement shall include clarifying language in the BYOD User Agreement for the expectation of privacy, requirements for litigation, e-discovery, and legal holds; and

(f) The BYOD User Agreement shall clearly state the expectations of the loss of personal data in the event a wipe of the device is required.

MD-05: NETWORK ACCESS
Agencies are to consider all personally owned and third-party owned (BYOD) network-capable mobile devices as untrusted and unsecure. Only State-owned and managed mobile devices shall be trusted and permitted to connect to internal agency networks and systems.

Guidelines: Agencies may implement guest wireless networks that are segmented from the agency's internal networks to provide network access for personally owned and third-party owned network capable mobile devices. Agencies should ensure users are aware of the prohibition against connecting personal devices to the internal agency networks and consider the use of 802.1X or other Network Access Control (NAC) strategies to enforce network security.

MD-06: CENTRALIZED MANAGEMENT
Agencies deploying or authorizing the use of mobile devices for State business purposes, regardless of whether the mobile device is owned by the State, its user, or a third-party, shall implement a centralized Mobile Device Management solution that is to be used to enforce the security controls and policies necessary to keep State information assets secure.

Guidelines: Centralized Mobility Management solutions may include Mobile Device Management (MDM), Mobile Application Management (MAM), or other similar solutions that allow for
enforcement of security controls necessary to protect mobile devices, mobile applications, and agency data stored, accessed, processed, or transmitted on mobile devices.

MDM solutions allow for the enforcement of technical security requirements via the installation of an MDM application on the device, which provides agency IT support personnel with the ability to manage the device. MAM solutions are less intrusive to the user than MDM solutions, especially for individuals using personally owned or third-party-owned devices, as MAM only provides agency IT support personnel with the ability to manage agency application(s), the application data, and application security on the device. Both MDM and MAM solutions allow for:

- Passcode enforcement;
- AD/LDAP integration;
- Application containerization and data encryption;
- Enforcement of data loss prevention (DLP) policies;
- Jailbreak detection;
- Management of agency and commercial applications used for State business purposes; and
- Inventory tracking.

**MD-07: ELIGIBLE MOBILE DEVICES**
Agencies shall only authorize the use of mobile devices for State business purposes that are capable of being managed by the agency’s centralized mobility management solution and implementing the technical security controls as required herein. Mobile devices that are incapable of being centrally managed, or of implementing the following technical controls, are not permitted to be used for State business purposes.

**MD-08: TECHNICAL SECURITY CONTROLS**
Asset custodians shall ensure the following technical security controls are implemented and enforced on all mobile devices used for State business purposes.

(a) Authentication - Logical access to the mobile devices and/or mobile applications that access agency data shall be controlled through the use of authenticators (passwords, biometrics, etc.);

(b) Authenticators - Where technically feasible, mobile device passwords shall, at a minimum, consist of 6 characters;

Guidelines: Modern mobile devices provide biometric and other advanced authentication mechanisms, in addition to the device password. Passwords shall be established for all mobile devices used for State business purposes. The use of a biometric or alternate authenticator by the device, after the password is implemented, is permitted;
(c) Auto-wipe - Where technically feasible, a mobile device shall automatically wipe its contents after 10 consecutive failed login attempts;

(d) Session Lock - Mobile devices are required to implement an inactivity locking mechanism to lock the device, and require re-authentication, after no more than five (5) minutes of inactivity;

(e) Jailbreaking/Rooting - Agencies shall enforce security controls, and the detection and prevention of their circumvention, through the use of the centralized mobile device management system. Mobile devices that have been jailbroken/rooted shall be denied access to State information assets;

Guidelines: The terms jailbreaking and rooting are commonly referred to as the modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator (e.g. to allow the installation of unauthorized software). Jailbreaking or rooting mobile devices used for State business purposes is prohibited;

(f) Encryption of Agency Information - All agency non-public information stored on mobile devices shall be encrypted in accordance with the Cryptographic Protection Policy contained in this Manual;

Guidelines: Modern smartphones and tablets generally offer full-device encryption as a default setting thereby protecting all data stored on them.

(g) Anti-Malware - Anti-malware software shall be implemented on all mobile devices, where supported:

   (1) Android mobile devices are required to have anti-malware software installed;

   (2) Windows mobile devices are required to have anti-malware software installed;

   and

   (3) The Apple iOS mobile devices are not currently capable of running anti-malware software, since no such software exists, based on the design of iOS;

(h) Operating System Security - where technically feasible, all mobile devices shall have the latest available operating system updates installed upon general release by the device or operating system manufacturer:

   (1) Agency asset custodians are to manage operating system updates/upgrades for State-owned devices as part of their change management processes;

   (2) Users of BYOD mobile devices shall be responsible for implementing operating system updates on their devices;

   (3) Mobile devices used for State business purposes shall allow for remote validation to download the latest security patches by Agency asset custodians; and

   (4) All mobile devices used for State business purposes shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier; and
Guidelines: Mobile device operating system updates/upgrades typically include security enhancements or patches in addition to new or enhanced features. Mobile devices that are incapable of running operating systems at vendor supported levels shall be prohibited from being used for State business purposes.

(i) Remote Wipe - All mobile devices permitted for State business use must have the capability, and be configured to allow, agency asset custodians to remotely wipe all agency non-public information.

Guidelines: This standard protects information on mobile devices if the devices are lost or stolen. On user-owned and third-party owned mobile devices the remote wipe should only purge agency information. Personal information and applications should not be wiped. Users should note that in some cases limiting the wipe execution to only agency data may not be possible.

**MD-09: INVENTORY**

Agencies shall:

(a) Maintain an inventory of all permitted mobile devices and mobile applications that are used for State business purposes;

(b) Permit only mobile devices that are authorized and enrolled in the agency’s centralized mobility management solution for State business use; and

(c) Record all changes to the status of these devices in the inventory.

Guidelines: Inventories should include the device manufacturer, model, operating system and patch levels, applications used for State business purposes, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD).

**MD-10: APPROVED APPLICATION STORES**

To mitigate the risks associated with the installation of rogue applications, agencies shall establish a documented and communicated list of approved application stores (e.g. State/Agency App Catalog, Apple Store, Google Play, etc.) through which mobile devices may obtain approved applications.

**MD-11: APPROVED APPLICATIONS**

Agencies are required to:

(a) Establish a documented and communicated list of approved applications that may be installed and used on mobile devices that are used for State business purposes;

(b) Establish a documented application validation process to test for device, operating system, and application compatibility issues; and
(c) Non-approved applications shall be prohibited from being installed on State-owned mobile devices or used for State business purposes, regardless of the ownership of the device.

Guidelines: Agency are to vet and ensure that approved applications do not introduce additional risks to the confidentiality, integrity, availability, and privacy of agency data or compromise the security of the device.

**MD-12: APPLICATION MANAGEMENT**

Where technically feasible, agencies shall manage all mobile applications used for State business at the latest vendor supported levels regardless of whether the applications are installed on State-owned, user-owned, or third-party owned mobile devices.

Guidelines: Agencies are to manage security-related updates/upgrades for all State-owned devices as part of their change management processes.

**MD-13: APPROVED CLOUD SERVICES**

Agencies are required to establish a documented and communicated list of approved cloud services that may be used with mobile devices used for State business purposes. The use of personal cloud services including, but not limited to email, file storage, etc., for State business purposes is not permitted.

Guidelines: The usage of personal email accounts, personal storage accounts, and other personal cloud services is not permitted for State business purposes.

**MD-14: BACKUP**

Agencies shall:

(a) Establish mechanisms and requirements to backup mobile devices in order to mitigate the risk of loss of agency information; and

(b) Prohibit the backing up of agency information to personal computers, personal storage devices, and personal cloud services.

**MD-15: SAFETY AND COMPLIANCE**

All usage of mobile devices must comply with State, Federal, and local laws in which the mobile device is operated.

**MD-16: TRAINING OF MOBILE DEVICE USERS**

Agencies shall ensure that managers, supervisors, and mobile device users receive security training, addressing at a minimum, the following subjects:

(a) The requirements as outlined herein;
(b) Compliance with legal, regulatory, and contractual requirements related to the use of mobile devices;
(c) The safe use of a mobile device, especially while driving;
(d) The potential risks to the agency’s information assets;
(e) Anti-malware awareness training, specific to mobile devices;
(f) The potential risks associated with the use of personally owned mobile devices and the agency’s limitations to support personally owned mobile devices;
(g) The use of approved application stores and applications;
(h) Protection of authenticators, such as passwords, personal identification numbers (PIN), and hardware tokens;
(i) The consequences for disabling, altering or circumventing the security configurations that protect agency information assets; and
(j) Security incident management and loss/theft of mobile device reporting procedures.

REFERENCES
The requirements established in the Mobile Device Management Policy have been derived from the following:

- NIST SP 800-53 Access Control (AC), Media Protection (MP), Physical and Environmental Protection (PE); and
- NIST CSF Identify/Asset Management (ID.AM), Protect/Access Control (PR.AC), Protect/Information Security Policies and Procedures (PR-IP).
PURPOSE
The purpose of the Network Security Policy is to ensure sufficient administrative, physical, and technical security controls are implemented to protect State networks and the information assets that reside within them.

KEY TERMS
Boundary Protection Device - A device with appropriate mechanisms that:

(i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or

(ii) provides information system boundary protection.

Defense-in-Depth - The coordinated use of multiple security countermeasures to protect the integrity of the information assets. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

NS-01: POLICY
Agencies shall implement defense-in-depth and least privilege strategies for securing the information technology networks that they operate. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, agencies shall:

(a) include protection mechanisms for network communications and infrastructure;

(b) include protection mechanisms for network boundaries;

(c) control the flow of information; and

(d) control access to State information systems,

while still providing acceptable functionality and performance necessary to effectively conduct State business operations.

This policy is supported by the following standards and guidelines.

NS-02: NETWORK MANAGEMENT
Unless otherwise specified by contract or written agreement:

(a) The New Jersey Office of Information Technology (NJOIT) shall be responsible for procuring, designing, managing, implementing, monitoring, and securing the State of New Jersey Garden State Network (GSN), that provides information technology and
telecommunications resources, including WAN aggregation, remote access, data center connectivity, and Internet services to Executive Branch Departments and Agencies;

(b) Executive Branch Agencies, whether independently or through a services agreement with NJOIT, shall be responsible for the development and implementation of network and telecommunications designs, processes, and technical security controls necessary to provide authorized access to agency technology resources, in accordance with the technical standards defined by NJOIT; and

(c) The NJOIT shall be responsible for the central management and allocation of the IP address space and Domain Name Services (DNS) used to provide network services to GSN entities.

Guidelines: The objective is to ensure the protection of information in networks and their supporting information processing facilities. Networks should be managed and controlled to protect information in systems and applications.

Consistent with Executive Order 225, the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term, agency includes OIT and all ancillary departments and agencies. Agencies must coordinate all network design, implementation, management, and operation with OIT to ensure security is accounted for throughout the GSN.

**NS-03: IDENTIFIED RESPONSIBILITY**
Agency CIOs, or their qualified designees, are identified as the final decision makers regarding the management of, changes to, updates to, or modifications of agency owned and/or managed networks and network devices, in accordance with the technical standards defined by NJOIT and the security requirements as defined by NJHSP and documented herein, or otherwise required by policy, statute, regulation, or contract.

**NS-04: DOCUMENTATION**
Agencies shall inventory all network devices in accordance with the Asset Management requirements set forth in this Manual. Inventory documentation must include the physical location of the devices and an agency point of contact who is responsible for the management of the network devices.

The following must be documented and maintained by agencies as part of the network documentation:

(a) Current-state and comprehensive network diagrams of the various network components, including routers, firewalls, switches, and VPNs;
(b) Network Access Points;
(c) Connectivity and the types of connectivity, if any, between the various networks;
(d) Data flows;
(e) Segregation of networks;
(f) IP address and naming schemes; and
(g) Routing tables.

**NS-05: GENERAL PHYSICAL SECURITY REQUIREMENTS**
All information assets used to manage, pass, or filter network traffic shall be physically secured to prevent unauthorized physical access.

(a) Agencies shall establish controls to manage all physical connections to agency networks;
(b) All physical connections shall be disabled when not in use; and
(c) Agencies shall establish procedures that require managers to notify agency network personnel when physical connections are no longer needed.

Guidelines: Unused physical connections can be disabled using various approaches including disabling the use of a port at the switch level.

**NS-06: LAYERED DEFENSES**
Agencies are required to implement a Defense-in-Depth (DiD) architecture placing information systems that contain sensitive information in an internal network zone, segregated from the DMZ and other untrusted networks.

Guidelines: Defense-in-Depth entails implementing multiple layers of security controls (defense) placed throughout the network system. The implementation of layered defenses with minimized interactions among security functions and non-looping layers (e.g., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

**NS-06.1: DENIAL OF SERVICE (DOS) PROTECTION**
Agencies shall implement controls and configure their network and systems architectures to limit the effects of denial of service attacks.

Guidelines: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.
Agencies should ensure their architectures and controls minimize the effects of the following types of DoS attacks:

- **Volumetric Attacks** – These attacks operate by sending more connection requests (such as transmission control protocol (TCP) synchronize or SYN messages) than can be processed by the target.

- **Application Layer Attacks** – A common type of application layer attack uses HTTP GET or HTTP POST requests to overwhelm a Web server. HTTP GET requests retrieve static content from Web servers and are easy to craft. HTTP POST requests retrieve more dynamic content and can be used to tie up processing power or generate large responses.

- **Reflection and Amplification Attacks** – These attacks target and exploit network protocols such as domain name system (DNS), character generation (CHARGEN) and network time protocol (NTP). Amplification attacks generate large responses from small requests; and reflection attacks use spoofing to direct unwanted responses to a target IP address.

- **Stealthy Attacks** - such as Slowloris, are designed to exhaust the resources of targeted web servers by sending partial HTTP requests at regularly timed intervals to keep connections open as long as possible. Eventually, the open connections will fill the web server’s maximum concurrent connection pool, denying additional connection attempts from legitimate users. The result is a stealthy, low bandwidth attack that disables a specific web server in a way that avoids triggering volumetric-based detection mechanisms.

**NS-06.2: PARTITIONING**

Where technically feasible, agencies shall configure systems to separate user functionality (including user interface services) from system management functionality. Separation may be accomplished through one or more of the following:

(a) Network segmentation;

(b) Different computers;

(c) Different central processing units;

(d) Different instances of the operating system;

(e) Different network addresses; or

(f) Other methods as appropriate.

Guidelines: System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is either physical or logical. Agencies implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network
addresses, virtualization techniques, or combinations of these or other methods, as appropriate.

**NS-06.3: GUEST NETWORKS**
If required for business needs, agencies shall implement secure guest networks such that guest network access is required to:

(a) Be limited to a separate network that is logically separated from the agency’s internal networks that host sensitive information and systems;
(b) Permit only authorized traffic between the guest environment and internal networks;
(c) Prevent direct access to agency internal network(s); and
(d) Guest access permission must be revoked after 24 hours.

Guidelines: Separate Virtual Local Area Networks (VLANs) for BYOD systems or other untrusted devices should be created. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly. In instances in which a contractor, using a system not managed by an agency, may need access to internal agency network systems, the use of VPN technologies should be used to prevent direct connections from the unmanaged device on the guest network to an internal network.

**NS-07: BOUNDARY PROTECTION**
Boundary protection is the comprehensive monitoring and control of communications within the “external boundary” of one’s overall information systems environment for purposes of detecting and preventing malicious, unauthorized communication via the use of numerous tools and utilizes (i.e. firewalls, routers, trusted data transmission tunnels, Intrusion Prevention and Intrusion Detection Systems (IPS/IDS), etc.). More specifically, boundary protection clearly distinguishes boundaries between external, untrusted networks from those deemed trusted and secure.

Agencies shall employ boundary protection mechanisms to separate system components directly supporting agency-defined missions and/or business functions. Agency network administrators are required to:

(a) Implement a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the internal network zone;
(b) Verify that the current network diagrams are consistent with the firewall configuration standards;
(c) Prohibit direct public access between the Internet and any sensitive system in an internal network;
(d) Restrict inbound and outbound traffic to that which is necessary for authorized business purposes;
(e) Limit the number of access points to the GSN to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;

(f) Ensure traffic flow policies are established and reviewed for each managed interface;

(g) Ensure the exceptions to Access Control Lists (ACLs) are approved documented and reviewed;

(h) Ensure private IP addresses and routing information are not disclosed to unauthorized parties; and

(i) Implement a firewall between any wireless networks and the internal network zones:

1. Verify that there are perimeter firewalls installed between any wireless networks and systems that store sensitive information; and

2. Configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the internal network zones.

Guidelines: Any unauthorized services or traffic should be blocked and an alert generated. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or sub-networks, cross-domain devices separating sub-networks, and encrypting information flows among system components using distinct encryption keys. The degree of separation provided varies depending upon the mechanisms chosen.

**NS-07.1: INTERNET ACCESS POINTS**

All Internet access points that provide connectivity between the GSN and the public Internet shall be procured, implemented, and managed throughout their lifecycle by the NJOIT. Agencies shall ensure the NJOIT is aware of any current or future plans for external network connections. The number of external network connections to the Garden State Network shall be limited and controlled.

Guidelines: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections. For more information, see https://www.dhs.gov/trusted-internet-connections.

**NS-07.2: SPLIT TUNNELING**

Where technically feasible, agencies are required to configure remote devices (e.g., laptop and notebook computers) to prevent “split tunneling”.

Guidelines: Agencies are to configure the remote devices to disable split tunneling and to prevent those configuration settings from being readily configurable by users. This standard is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.
Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of agency data. VPNs provide a means for allowing non-remote communications paths from remote devices.

**NS-07.3: INTERNAL NETWORK ADDRESS SPACE**
Agencies are required to configure systems to prevent the disclosure of private IP addresses and routing information to unauthorized parties. Methods to obscure IP addressing may include, but are not limited to:

(a) Network Address Translation (NAT)/Port Address Translation (PAT);
(b) Placing systems behind proxy servers/firewalls or content caches;
(c) Removing or filtering route advertisements for private networks that employ registered addressing; and
(d) Using internal use RFC1918 address space instead of registered addresses.

**NS-08: DATA FLOW ENFORCEMENT - ACCESS CONTROL LISTS (ACLS)**
Agencies shall deploy and configure firewalls and routers in order to restrict connections between untrusted networks and any system components within the network by the following means:

(a) Implement Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to only that which is necessary, as defined by a business justification;
(b) Assign privileges to individuals based on job classification and function (Role-Based Access Controls);
(c) Utilize “deny-all” setting by default and only allow by exception;
(d) Secure and synchronize router and firewall configuration files;
(e) Position perimeter firewalls between wireless networks and internal networks;
(f) Document business justification for the use of all services, protocols, and ports allowed;
(g) Use Demilitarized Zones (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
(h) Inbound Internet traffic shall be limited to IP addresses within the DMZ;
(i) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network;
(j) Prohibit unauthorized outbound traffic to the Internet;
(k) Implement stateful inspection (dynamic packet filtering);
(l) Segment internal trusted networks from other untrusted networks; and
(m) Prohibit private IP addresses and routing information from being disclosed to unauthorized parties.

Guidelines: Not all firewalls and routers have the functionality for the running configuration to be different than the configuration loaded at startup. However, if the functionality exists, the startup configuration must be synchronized with the correct running configuration so that a reboot of the device will not degrade network security.

**NS-08.1: DENY TRAFFIC BY DEFAULT AND ALLOW TRAFFIC BY EXCEPTION**

Agencies shall configure managed interfaces to deny network traffic by default and only allow network traffic by exception (e.g. deny all, permit by exception).

Guidelines: Denying traffic by default and only allowing by exception applies to both inbound and outbound network communications traffic. A deny all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

**NS-08.2: REVIEWS OF FIREWALL AND ROUTER RULE SETS**

Agency CISOs are responsible for implementing reviews of firewall and router rule sets at least annually or as required by applicable compliance requirements to ensure least privileges and industry-recognized leading practices are being followed.

Guidelines: Human reviews regarding information flow enforcement decisions are necessary when systems are not capable of making such flow control decisions or when agencies deem human reviews necessary. Business units are responsible for defining policy filters for all cases where automated flow control decisions are not possible or deemed to be not sufficient. Human reviews of firewall rule sets may be required to be performed more frequently to satisfy compliance requirements such as PCI-DSS.

**NS-09: INFORMATION SYSTEM CONNECTIONS**

Only devices that are owned or managed by State agencies and meet baseline hardening standards are allowed to connect directly to agency internal network(s).

Guidelines: Third-party remote access is allowed only through approved site-to-site VPN connections or through approved remote desktop-based connections. NJOIT is the arbiter of approved remote desktop software. Software that provides remote desktop-based connections not approved by NJOIT is prohibited.

**NS-09.1: SENSITIVE INFORMATION SYSTEMS**

Agencies shall prohibit the direct connection of a sensitive information system to an external network without the use of a boundary protection device.
Direct connections of agency systems to the Internet are:

(a) Allowed for mobile devices being operated outside of State facilities, as long as the mobile devices have host-based antimalware software installed and the host-based firewall is active;

(b) Prohibited for systems residing on an agency’s internal network(s); and

(c) Direct connections inbound or outbound for traffic between the Internet and sensitive data environments are prohibited.

Guidelines: Agencies typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., firewalls) mediate communications (e.g., information flows) between sensitive agency systems and external networks.

**NS-09.2: RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS**

Network and Firewall Administrators shall establish and manage firewall and router configuration standards to prohibit direct public access between the Internet and any system component on internal networks that includes, but is not limited to:

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;

(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ;

(c) Anti-spoofing measures shall be implemented to detect and block forged source IP addresses from entering the network;

(d) Stateful inspection (dynamic packet filtering) must be implemented;

(e) System components that store sensitive information must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; and

(f) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties.

Guidelines: Agencies typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (e.g., information flows) between internal systems and external networks.

Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT);
- Placing servers containing sensitive data behind proxy servers/firewalls;
- Removal or filtering of route advertisements for private networks that employ registered addressing; or
- Internal use of RFC 1918 address space instead of registered addresses.
NS-10: SECURITY FUNCTION ISOLATION

Agencies are required to implement isolation techniques to prevent functions that require different security levels from co-existing on the same server. Isolation techniques include, but are not limited to:

(a) Implementation of only one primary function per server to prevent functions that require different security levels from co-existing on the same server, where technically feasible;

(b) Firewall and router configurations must be configured to restrict connections between untrusted networks and any system components in an agency’s trusted, internal network;

(c) Firewalls must be installed at all connections from an internal to any other internal or external network;

(d) Demilitarized Zones (DMZs) must be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;

(e) Networks must be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices;

(f) Switched network technology is to be utilized, when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic;

(g) Trust relationships must be strictly avoided between information resources with different risk profiles; and

(h) Information resources with higher protection requirements for confidentiality must not have a trusted relationship with a system that has lower protection requirements.

Guidelines: The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. An “untrusted network” is any network that is external to the networks belonging to the agency and/or one that is out of the agency's ability to control or manage. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

NS-10.1: HOST-BASED PROTECTION

Agencies are required to implement host-based firewall controls or install equivalent functionality on all Internet-accessible mobile devices or computers. The host-based firewalls are to be configured to deny all network traffic not necessary to conduct business. Host-based firewalls are to be configured in such a manner to prevent alteration by users.

Guidelines: Host-based boundary protection mechanisms include, for example, host-based firewalls. System components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.
NS-10.2: SEPARATE SECURITY MANAGEMENT SUBNETS
As technically feasible, agencies shall isolate information security technologies, tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks.

Guidelines: Physically separate subnetworks with managed interfaces are used to isolate computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.

NS-10.3: VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION
Agencies shall enable Virtual Local Area Networks (VLANs) on all network switches to segment networks based on the security categorization of the information stored on the systems within a network segment in order to limit an attacker’s ability to laterally move and compromise neighboring systems.

Guidelines: Agencies should locate all sensitive information on separated VLANs with firewall filtering to ensure that only authorized individuals are able to communicate only with systems necessary to fulfill their specific responsibilities.

NS-11: NETWORK DISCONNECT/TIMEOUT
Agencies shall configure systems to terminate sessions and require users to re-authenticate to re-activate a terminal or remote session if a session has been idle for more than fifteen (15) minutes.

Guidelines: This applies to both internal and external networks and local and remote connections.

NS-12: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)
Network Intrusion Detection Systems (NIDS) and/or Intrusion Prevention Systems (NIPS) are required to be implemented at the perimeter of the GSN and all critical points in the network in order to monitor all traffic, prevent intrusions into agency networks, and alert information security personnel to suspected compromises within the network.

All intrusion detection and prevention engines shall be configured to automatically update their signatures in order to maintain currency with emerging threats.

Guidelines: Critical points in the network may include but are not limited to boundaries between agencies on the GSN, segmented networks that host highly sensitive information, and connections between wireless networks and internal agency networks.

Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise
types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.

Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.

**NS-12.1: DMZ NETWORK - IDS/IPS**

Network administrators are required to deploy Network-based Intrusion Detection/Prevention Systems (NIDS/NIPS) on Internet and extranet DMZ network segments and networks.

**NS-12.2: WIRELESS NETWORKS – WIRELESS INTRUSION DETECTION/PREVENTION SYSTEMS**

As technically feasible, network administrators are required to deploy Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) on wireless network segments to identify:

(a) Rogue wireless devices; and

(b) Attacks coming from the wireless network(s).

Guidelines: Dedicated WIDS/WIPS security technologies build upon traditional network IDS/IPS technologies by adding features that identify and prevent intrusion attempts unique to wireless networks. In addition to WIDS/WIPS, all wireless traffic should be monitored and processed by a firewall as traffic passes into the wired network.

**NS-13: SAFEGUARDING DATA OVER OPEN NETWORKS**

Data that traverses public networks shall be appropriately protected from fraudulent activity, unauthorized disclosure, or modification. To safeguard sensitive data during transmission, asset custodians are required to ensure the following:

(a) Only trusted keys and certificates are accepted;

(b) Strong cryptography and security protocols are used to safeguard sensitive cardholder data during transmission over open, public networks. Examples of technologies that support this requirement include, but are not limited to:

(1) Transportation Security Layer (TLS);

(2) IP Security (IPSEC);

(3) Secure Shell (SSH); and
(4) Secure File Transfer Protocol (SFTP) / File Transfer Protocol - Secure (FTP-S); and

c) Wireless networks transmitting sensitive data or connected to sensitive networks, use industry-recognized leading practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission.

Guidelines: All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted. Examples of open, public networks that are considered to be untrusted include but are not limited to:

- The Internet;
- Wireless technologies;
- Global System for Mobile communications (GSM); and
- General Packet Radio Service (GPRS).

Trusted certificates are issued by Certificate Authorities (CA). The certificates verify the identification of a digital identity of an entity and allow for secure connections on the Internet. Trusted certificates are essential in the implementation of a Public-Key Infrastructure (PKI). Additional guidance regarding cryptographic controls can be found in the Cryptographic Protection Policy in this manual.

**NS-14: REMOTE ACCESS**

The NJOIT at the direction of the State CTO is responsible for defining allowed methods of remote access to systems and services internal to the Garden State Network (GSN). The use of remote control software shall be strictly controlled and shall be prohibited from connecting into agency networks or to agency network assets from a public network without approval from the agency CISO, the Agency SVR, and the State SVR, and the State CISO. All remote access to internal agency assets shall adhere to all remote access requirements as documented in the Access Management Policy.

NJOIT shall be responsible for:

(a) Documenting allowed methods of remote access to the GSN;

(b) Establishing usage restrictions and implementation guidance for each allowed remote access method;

(c) Monitoring for unauthorized remote access to information systems;

(d) Authorizing remote access to information systems prior to connection;

(e) Enforcing requirements for remote connections to information systems;

(f) Using cryptography to protect the confidentiality and integrity of remote access sessions;

(g) Automatically disconnecting remote access sessions after a period of inactivity; and
(h) Immediately deactivating vendor and business partner remote access when it is no longer needed.

Guidelines: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless.

All agency devices remotely logging into the agency’s internal network should be managed by the agency allowing for remote control of the device(s) configuration, installed software, and patch levels. Third-party devices (e.g., subcontractors/vendors), shall be required to meet the State’s security standards as stated within this Manual for access to the agency networks. The use of Network Access Control (NAC) technologies should be considered to enforce security requirements for all devices connecting to internal networks.

**NS-15: DOMAIN NAME SERVICE (DNS) RESOLUTION**

Agencies shall use trusted sources as defined by NJOIT for authoritative DNS queries to prevent DNS spoofing attacks and enable DNS query logging to detect hostname lookup for known malicious Command & Control (C2) domains. Agencies responsible for implementing and managing the Domain Name System (DNS) are required to:

(a) Ensure DNS Servers providing name/address resolution service are fault tolerant and implement internal/external role separation;

(b) Ensure primary and secondary authoritative DNS servers are on separate subnets at separate locations;

(c) Ensure DNS servers with an internal role only process name/address resolution requests from internal clients;

(d) Ensure DNS servers with an external role only process name/address resolution requests from external clients; and

(e) Configure internal DNS queries to use recursive or cached name resolution.

Guidelines: NJOIT is responsible for managing the State’s internal DNS infrastructure. Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, OIT must employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server.

For role separation, DNS servers with internal roles should only process name and address resolution requests from within agency internal networks (e.g., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to the agency networks (e.g., the Internet). Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted
validation providers. Systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

**NS-16: WIRELESS NETWORKING**

For wireless networking:

(a) Agency CIOs and CISOs are responsible for

1. Establishing usage restrictions and implementation guidance for wireless access;
2. Monitoring for unauthorized wireless access to the system;
3. Authorizing wireless access to systems prior to connection; and
4. Enforcing requirements for wireless connections to systems.

(b) Wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection; and

(c) Wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).

Guidelines: Wireless technologies include, but are not limited to:

- Microwave;
- Satellite;
- Packet radio (UHF/VHF);
- 802.11x; and
- Bluetooth.

**NS-16.1: AUTHENTICATION AND ENCRYPTION**

Agencies implementing wireless networks are required to ensure industry-recognized leading practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted.

Guidelines: Refer to the Center for Internet Security (CIS) Benchmarks and vendor documentation for the proper security configurations of Wireless Access Points (WAPs) and supported encryption strength.

**NS-16.2: DISABLE WIRELESS NETWORKING**

In sensitive environments, asset custodians are required to disable wireless networking capabilities in systems that do not have a legitimate need to have wireless network access.

Guidelines: Disabling wireless connectivity may be through least privileges in the operating system environment or through password protecting the system BIOS. Similar restrictions may be used to restrict access to only authorized networks.
NS-16.3: CONFIGURATION OF WIRELESS COMMUNICATIONS

Asset custodians are required to attempt to confine the wireless transmission boundary to within the geographic confines of agency facilities through:

(a) Proper placement of Wireless Access Points (WAPs);
(b) Limiting the output / transmission power of the WAPs;
(c) Disabling peer-to-peer wireless network capabilities on wireless clients; and
(d) Disabling wireless peripheral access of devices (e.g., Bluetooth), unless such access is required for a documented business need.

Guidelines: Actions that may be taken by NJOHSP to confine wireless communications to organization-controlled boundaries include, for example:

- Reducing the power of wireless transmissions such that the transmissions cannot transit physical perimeters of organizations;
- Employing measures to control wireless emanations (e.g., TEMPEST); and
- Configuring wireless accesses such that the accesses are point-to-point in nature.

NS-16.4: ROGUE WIRELESS DETECTION

Agency asset custodians and information security personnel are required to implement a process to test for the presence of Wireless Access Points (WAPs) that includes:

(a) Detecting and identifying all authorized and unauthorized wireless access points at least once every ninety (90) days;
(b) Maintaining an inventory of authorized WAPs including a documented business justification; and
(c) Implementing incident response procedures in the event unauthorized WAPs are detected.

Guidelines: Unauthorized (e.g., rogue) access points should be deactivated. Detection methods must be sufficient to detect and identify both authorized and unauthorized devices. Methods that may be used in the rogue WAPs (802.11) detection process includes, but are not limited to:

- Wireless network scans,
- Physical/logical inspections of system components and infrastructure,
- Network Access Control (NAC); or
- Wireless Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

NS-17: DATA LOSS PREVENTION (DLP)

Where technically feasible, agencies shall deploy Data Loss Prevention (DLP) technologies to:
(a) Monitor for sensitive information (e.g., Sensitive Personally Identifiable Information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries; and

(b) Block such transfers while alerting information security personnel.

Guidelines: DLP strategies include implementation at the perimeter of the GSN via email and web content filtering technologies, as well as at individual agency endpoint (laptops, workstations, servers). The NJCCIC manages the Executive Branch’s enterprise mail filter solution that includes DLP capabilities. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action is taken to address them.

**NS-18: INTERNET PROXY**

Agencies shall prohibit direct public access between the Internet and any system on their internal networks. Agencies shall implement network-based URL filters that limit a system’s ability to connect to prohibited websites, based on content and/or reputation:

(a) Agencies managing web filtering technologies shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available;

(b) Uncategorized sites shall be blocked by default;

(c) Agencies are required to develop policies that document permitted and prohibited web content categories for agency personnel;

(d) Agencies shall prohibit access to website content that is prohibited by State or federal law, Executive Orders, compliance regulations, and State or agency policies; and

(e) This filtering shall be enforced for all systems, whether the system is connected to agency networks or networks external to the GSN.

Guidelines: Common categories of website content that is to be blocked include, but are not limited to, sites containing illegal content, malware, hacking materials, anonymizers and proxy avoidance materials, pornography and other adult materials, and hate sites. Agency policies should provide personnel with guidance on the use of or access to other categories of websites including social media, chat, shopping, etc., that may impact an employee’s productivity or compliance with State and agency policies.

The proxy server should support decrypting network traffic, logging individual TCP and UDP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Agencies should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.
REFERENCES:
The requirements established in the Network Security policy have been derived from following:

- NIST SP 800-53 Secure Communications (SC), Access Control (AC); Security Assessment and Authorization (CA)
- NIST CSF Protect/Access Control (PR-AC). Protect/Protective Technologies (PR-PT).
PURPOSE

The purpose of the Cloud Security Policy is to establish security requirements that govern the use of private, public, and hybrid cloud environments by State of New Jersey Executive Branch Departments and Agencies, and to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed.

KEY TERMS

Application Program Interface (API) - An API specifies how some software components should interact with each other. In addition to accessing databases or computer hardware, such as hard disk drives or video cards, an API can be used to ease the work of programming graphical user interface components. In practice, many times an API comes in the form of a library that includes specifications for routines, data structures, object classes, and variables. In some other cases, notably for SOAP and REST services, an API comes as just a specification of remote calls exposed to the API consumers.

Cloud Access Security Broker (CASB) - consist of on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, and malware detection/prevention.

Cloud Computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Cloud Service Provider - is an entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, such as NJOIT, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

Hypervisor - also called the virtual machine monitor (VMM), is software that manages and controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards. The hypervisor can partition the system’s
resources and isolate the guest OSs so that each has access to only its own resources, as well as possible access to shared resources such as files on the host OS. Also, each guest OS can be completely encapsulated, making it portable. Some hypervisors run on top of another OS, which is known as the host operating system.

**Infrastructure as a Service** - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

**Platform as a Service** – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

**Service Level Agreement (SLA)** - Defines the specific responsibilities of the service provider and sets the customer expectations.

**Software as a Service** - The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

**Virtualization** - is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM).

**Virtual Private Cloud (VPC)** - is an on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources.

**CL-01: POLICY**
Agencies shall proactively manage risk in all of its private and public cloud environments through secure architectural decisions that align with NJOIT’s technology architecture strategy and provide continuous oversight of third-party responsibilities for keeping the environments both secure and efficient.

This policy is supported by the following standards and guidelines.
CL-02: CLOUD ACQUISITION AND DEVELOPMENT

Agencies shall:

(a) Follow all NJOIT and Department of Treasury, Division of Purchase and Property (DPP) requirements in the procurement and acquisition of cloud computing services;

(b) Ensure cloud computing providers meet or exceed the security control requirements as documented in the Cloud Security Alliance’s Cloud Controls Matrix, version 3.01;

(c) Where there is a requirement to comply with Federal Risk and Authorization Management Program (FedRAMP) requirements, ensure cloud computing providers meet or exceed the applicable FedRAMP Low, Moderate, or High thresholds;

(d) Ensure cloud computing providers (internally and externally) meet or exceed the requirements set forth in this Manual regarding information security, as well as, all applicable State and Federal laws, regulations, and agency-specific information security policies;

(e) Annually review Cloud service provider’s cybersecurity attestation for compliance to required infrastructure compliance certification; and

(f) As feasible, obtain approval from the Cloud service provider to perform vulnerability scans against infrastructure used by the State of New Jersey.

Guidelines: The Cloud Security Alliance (CSA) should be referenced for security-related architectural questions for cloud deployments. The CSA provides industry-leading practice for:

- Software as a Service (SaaS);
- Infrastructure as a Service (IaaS); and
- Platform as a Service (PaaS).

CL-03: CLOUD PROVIDERS

For cloud providers that maintain shared hosting environments, agencies are required to:

(a) Maintain a comprehensive list of those service providers with whom they contract, including all applicable Service Level Agreements (SLAs);

(b) Require that the cloud providers, at a minimum, comply with information security requirements documented in the Statewide Information Security Manual, and employ appropriate security controls in accordance with State and Federal laws, as well as all applicable regulatory and contractual requirements;

(c) Define and document oversight roles and responsibilities for both the cloud provider and the Agency regarding external information system services and information security;

(d) Perform a review of the information system and information security services provided for acceptable service levels;
(e) Conduct a risk assessment regarding the outsourcing of services to a cloud provider; and
(f) Monitor security control compliance by those external service providers.

Guidelines: Cloud providers typically provide tenants (customers) with cloud services within a shared hosting environment, meaning multiple customers’ data is stored on one server. Agencies must ensure that the cloud provider provides affords protection for each tenant’s data and processing environment such that another customer’s insecure functions do not impact the security of the Agency’s environment.

**CL-04: CLOUD SECURITY ARCHITECTURE**

The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces (e.g., API) must be conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations. Minimum expectations for cloud-based architecture includes, but is not limited to:

(a) Services running in a cloud must follow the principles of least privilege;
(b) Isolation between various security zones must be guaranteed using layers of firewalls (e.g., cloud firewall, hypervisor firewall, guest firewall and application container);
(c) Firewall policies in the cloud must comply with trust zone isolation standards based on information sensitivity;
(d) Applications must use end-to-end transport level encryption (e.g., TLS or IPSEC) to secure data in transit between applications deployed in the cloud as well as to the agency;
(e) Applications must externalize authentication and authorization to trusted security services;
(f) If Single Sign-On (SSO) is used, it must support industry-recognized protocols (e.g., SAML 2.0);
(g) Implementation of multi-factor authentication for all user and administrator access to the cloud service;
(h) Data masking and encryption must be employed based on data sensitivity aligned with the Security Categorization Policy, and all applicable State and Federal laws and regulations;
(i) Applications in a trusted zone must be deployed on authorized, standard Virtual Machine (VM) images;
(j) Industry standard VPN protocols such as SSH, TLS and IPSEC must be employed when deploying Virtual Private Cloud (VPC); and
(k) Security monitoring in the cloud must be integrated with existing Agency and/or NJCCIC security monitoring tools (e.g., API feeds to Agency or enterprise SIEM).
Guidelines: The Cloud Security Alliance (CSA) should be referenced for security-related architectural questions for cloud deployments. The CSA provides industry-leading practice for:

- Software as a Service (SaaS);
- Infrastructure as a Service (IaaS); and
- Platform as a Service (PaaS).

Additional information and requirements regarding security monitoring can be found in the Continuous Monitoring Policy.

**CL-05: SECURITY MANAGEMENT SUBNET**

Where technically feasible, agencies shall ensure cloud providers:

(a) Use secure protocols; and

(b) Where technically feasible, separate the management function of the network from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Guidelines: A good security practice is to separate network management functions (network management data traffic) from business use (user data traffic).

**CL-06: APPLICATION PROGRAM INTERFACE (API) SECURITY**

Agencies shall ensure cloud providers use open and published APIs to:

(a) Ensure support for interoperability between components; and

(b) Facilitate migrating applications.

Guidelines: Agencies should refer to the Open Web Application Security Project (OWASP) API Security Project for guidance regarding API security.

**CL-07: SECURITY ROLES AND RESPONSIBILITIES**

Agencies shall explicitly define roles and responsibilities of the cloud service provider and Agency team for operations security including, patch management, incident response, etc.

**CL-08: VIRTUAL MACHINE IMAGES**

Agencies shall development and implement processes and safeguards that require the cloud service provider to:

(a) Configure virtual machine images in accordance with the requirements documented in this Manual and with all applicable State and Federal laws, and regulations; and

(b) Ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running).
Guidelines: The results of a change or move of a virtual machine image and the subsequent validation of the image's integrity must be immediately available to agencies through electronic methods (e.g. portals or alerts or emails). For more information on managing virtual machine images please refer to the Cloud Security Alliance’s Cloud Controls Matrix.

**CL-09: MULTI-TENANT ENVIRONMENTS**

Multi-tenant applications, infrastructure systems, and network components, must be designed, developed, deployed, and configured such that cloud provider and Agency user access is appropriately segmented from other tenant users, based on the following considerations:

(a) The established State of New Jersey information security policies contained in this Manual;

(b) More stringent agency-specific policies;

(c) Compliance with State and Federal statutory, regulatory and contractual compliance obligations; and

(d) Isolation of business-critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and higher levels of assurance.

**CL-10: DATA HANDLING AND PORTABILITY**

Agencies shall ensure cloud providers:

(a) Use secure network protocols for data transmission and to manage cloud-based services; and

(b) Provide agencies with all structured and unstructured data in the cloud environment upon request, in an industry-standard format (e.g., .doc, .xls, .pdf, etc.).

**CL-11: STANDARDIZED VIRTUALIZATION FORMATS**

Agencies shall require that cloud providers:

(a) Use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF, OVA, VMDK, BOX, etc.) to help ensure interoperability; and

(b) Have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for Agency review.

**CL-12: MOBILE DEVICE ACCESS**

Agencies shall implement policies, processes, and safeguards to ensure:

(a) All cloud-based services used by the Agency to conduct State business are authorized;

(b) Only authorized users, devices, and networks are permitted to access cloud services provided by the Agency;

(c) All cloud-based services used by the Agency and accessed by Agency users via mobile and/or BYOD devices are pre-approved for usage and storage of Agency data; and
(d) All mobile device usage is compliant with the Mobile Device Management Policy requirements as documented in this Manual.

**CL-13: GEOLOCATION REQUIREMENTS**

Agencies are required to ensure Cloud providers maintain all agency information within the United States.

Guidelines: The location of information processing, information/data storage, or information system services that are critical to the State can have a direct impact on the ability of agencies to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. For example, agencies should ensure that data/information storage locations are restricted to United States locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in the case of digital security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols outside the United States, in the locations where processing and storage occur and/or the locations from which information system services emanate.

**CL-14: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS**

Agencies shall:

(a) Ensure all public cloud providers meet or exceed the requirements for the storage of sensitive data as documented in this Manual and all applicable State and Federal laws, regulations, and contract obligations;

(b) Implement strong encryption (e.g., AES-256 or as guided by the State CISO, which is to be guided by emerging threats and vulnerabilities found with regards to any cryptographic algorithm in place.) in open/validated formats and standard algorithms;

(c) Prohibit the storage of cryptographic keys in public cloud environments (e.g., at the cloud provider in question); and

(d) Implement the principle of separation of duties for key management and key usage.


**REFERENCES**

The requirements established in the Cloud Security Policy have been derived from the following references:

- NIST SP 800-53: Systems and Services Acquisition (SA), Access Control (AC), System and Information Integrity (SI), System and Communications Protection (SC);
• NIST CSF: Identify – Business Environment (ID-BE); Identify – Governance (ID-GV); Identify – Supply Chain (ID-SC);

• NIST Special Publication (SP) 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*

• Cloud Security Alliance, *Cloud Computing Matrix v3.01*; and

• Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in cloud computing, v4.0*. 
CHANGE MANAGEMENT (CH)

PURPOSE
The purpose of the Change Management Policy is to establish controls required to ensure change is managed effectively. Change management provides agencies with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security.

KEY TERMS
None. See Glossary in Appendix B for a full list of key terms.

CH-01: POLICY
All technology changes to production environments must follow a standard process to reduce the risk associated with change. Agencies shall involve key business stakeholders in the change process to ensure changes are appropriately tested, validated, and documented before implementing any change on a production network.

This policy is supported by the following standards and guidelines.

CH-02: CONFIGURATION CHANGE CONTROL
Asset custodians and data/process owners are required to follow change control processes and procedures for all changes to system components:

(a) Utilize separate environments for development/testing/staging and production;

(b) Utilize a separation of duties between development/testing/staging and production environments and personnel;

(c) Prohibit the use of sensitive information (e.g., SSNs, Payment Card Numbers, etc.) for use within a testing or development environment;

(d) Remove test data and accounts before production systems become active / go into production;

(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following:
   1. Documentation of impact;
   2. Documented change approval by authorized parties; and
   3. Functionality testing to verify that the change does not adversely impact the security of the system.

(f) Back-out procedures; and
(g) Upon completion of significant change, all relevant compliance requirements, such as vulnerability scans, must be completed for all new or changed systems and networks, and relevant security documentation updated as applicable.

Guidelines: Configuration change controls for agency systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

CH-03: STAKEHOLDER NOTIFICATION OF CHANGES
Data/process owners are required to establish and maintain procedures to inform key stakeholders of system changes that affect agency operations or commitments.

CH-04: SECURITY IMPACT ANALYSIS FOR CHANGES
Change control processes and procedures must be followed for all changes to system components. From within a test environment, asset custodians are required to test proposed changes specifically to assess the security functions of the information system(s) to verify that those functions are:

(a) Implemented correctly;
(b) Operate as intended; and
(c) Meet the security requirements for the system.

Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The analysis process should include a review of the following:

(d) Separate development/test and production environments;
(e) Separation of duties between development/test and production environments;
(f) Production data (live data) is not used for testing or development; and
(g) Removal of test data and accounts before production systems become active.

CH-05: SECURITY FUNCTIONALITY VERIFICATION
Asset custodians are required to validate that security-related controls (e.g., anti-malware software) are operational after significant changes are implemented.

Guidelines: After major changes or software upgrades, it is recommended to test security-related tools to ensure the change did not disable the functionality of the security tool. An example of
security functionality verification is the European Institute of Computer Anti-virus Research (EICAR) Standard Anti-Virus Test File, which is used to ensure anti-malware software is properly detecting and removing threats. More information about EICAR can be found at: http://www.eicar.org/86-0-Intended-use.html. Alternatively, agencies may contact the NJCCIC to obtain a copy of the EICAR anti-virus test file.

REFERENCES
The requirements established in the Configuration Management policy have been derived from the following:

- NIST SP 800-53 Configuration Management (CM), System and Information Integrity (SI), Access control (AC); and
- NIST CSF Protect/Information Protection Policies and Procedures (ID.PR), Protect/Access Control (PR.AC).
INFORMATION ASSET MAINTENANCE (MA)

PURPOSE
The purpose of the Information Asset Maintenance policy is to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures.

KEY TERMS
Information Asset – An information asset is any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

MA-01: POLICY
In order to minimize risk from evolving threats, the periodic and ongoing maintenance and upgrades of agency information assets shall be performed and governed accordingly.

This policy is supported by the following standards and guidelines.

MA-02: MAINTENANCE OPERATIONS
Agencies are required to create, document and implement maintenance procedures to conduct maintenance operations for their information assets.

Guidelines: Information assets should be correctly maintained to ensure continued availability and integrity. Within an agency, the responsibility for conducting maintenance operations usually falls to asset custodians and business/information process owners.

MA-03: CONTROLLED MAINTENANCE
Agencies are required to:

(a) Schedule, perform, document, and review records of maintenance and repairs on systems in accordance with manufacturer or vendor specifications and agency requirements;

(b) Control all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location;

(c) Keep maintenance records for information systems that include:
   1. Date and time of maintenance;
   2. Name(s) of the individual(s) performing the maintenance;
   3. Name of escort, if necessary;
4. A description of the maintenance performed; and

5. A list of equipment removed or replaced (including identification numbers, if applicable);

(d) Require explicit management approval and appropriate documentation for the removal of systems or system components from State facilities for off-site maintenance or repairs;

(e) Sanitize equipment to remove all information from associated media prior to removal from State facilities for off-site maintenance or repairs; and

(f) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Guidelines: This addresses the cybersecurity aspects of the system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or non-local entity (e.g., in contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers.

Escort information may be required to be documented if the maintenance is performed by a third-party requiring an escort within the State facility. When using third-parties who require an escort to perform system maintenance, agencies should inspect all maintenance tools carried into agency facilities by maintenance personnel for obvious improper modifications or indications that proper maintenance is not being performed.

**MA-04: TIMELY MAINTENANCE**

Agencies are required to:

(a) Obtain maintenance support and spare parts for critical systems and key information technology components within defined Service Level Agreements (SLAs); and

(b) Conduct maintenance in a timely manner to minimize downtime and business disruption.

Guidelines: Agencies should document the assets that result in increased risk to operations in the event of a loss of functionality and prioritize the maintenance of those assets. Security-critical components include, for example, firewalls, routers, intrusion detection and prevention systems, and authentication servers.

**MA-05: REMOTE MAINTENANCE**

Agencies are required to:

(a) Authorize, monitor, and control non-local maintenance and diagnostic activities;

(b) Allow the use of non-local maintenance and diagnostic tools only in accordance with policy and standards;
(c) Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
(d) Maintain records of non-local maintenance and diagnostic activities; and
(e) Terminate all sessions and network connections when non-local maintenance is completed.

Guidelines: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the system or system component and not communicating across a network connection. Non-local maintenance should require authenticators that are resistant to replay attacks and employ multifactor authentication in accordance with the requirements documents in the Identity and Authentication Policy.

**MA-06: MAINTENANCE PERSONNEL**

Agencies are required to:

(a) Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel; and
(b) Ensure that personnel performing maintenance have required access authorizations or designate specific personnel with required access authorizations and technical competence necessary to supervise the maintenance when maintenance personnel do not possess the required access authorizations.

**REFERENCES**

The requirements established in the Information Asset Maintenance policy have been derived from the following:

- NIST SP 800-53 System Maintenance (MA); and
- NIST CSF Protect/Maintenance (PR-MA).
THREAT MANAGEMENT (TM)

PURPOSE
The purpose of the Threat Management Policy is to establish a formalized mechanism to collect and disseminate actionable threat intelligence, thereby providing agencies with the information necessary to effectively manage risk associated with new and emerging threats to State information assets and operations.

KEY TERMS
None. Please see Glossary in Appendix B for a complete list of key terms

TM-01: POLICY
The Director of the New Jersey Cybersecurity and Communications Cell (NJCCIC) shall establish and operate an Information Sharing and Analysis Organization (ISAO) that acts as the State clearinghouse for threat intelligence and information sharing. The NJCCIC:

(a) Liaises with the National Cybersecurity and Communications Integration Center within the US Department of Homeland Security, other federal agencies, and other public and private sector entities on issues relating to cybersecurity;

(b) Coordinates cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among State Government departments and agencies;

(c) Coordinates information sharing related to cybersecurity risks, warnings, and incidents, and provides support on cybersecurity incident response and cybercrime investigations;

(d) Provides information and recommends best practices on cybersecurity and resiliency measures to agencies, including those for information security and data protection; and

(e) Develops and implements a cybersecurity threat information exchange.

This policy is supported by the following standards and guidelines.

TM-02: THREAT AWARENESS PROGRAM
The Director of the NJCCIC and his/her designated representatives are responsible for establishing and implementing a formal threat awareness program that:

(a) Identifies the New Jersey State Government’s Departments’ and Agencies’ programs of work and the information systems that support them; and

(b) Communicates agency-specific threat information to each agency so that they can be aware of threats related to their programs of work, information systems, and threats that may impact organizations and the individuals they serve.
TM-03: THREAT INTELLIGENCE

Agencies shall ensure individuals within the agencies who are responsible for Information Technology and Information Security:

(a) Register as members of the New Jersey Cybersecurity and Communications Integration Cell;

(b) Subscribe to information security intelligence and information services in order to stay aware of emerging threats and vulnerabilities; and

(c) Use the information gained from these subscriptions to update their security posture and vulnerability and patch management activities, as applicable.

Guidelines: The NJCCIC acts as the State’s clearinghouse for threat intelligence and produces intelligence products including, but not limited to: alerts, bulletins, and best practices. Individuals can find NJCCIC registration information at: [https://www.cyber.nj.gov/members](https://www.cyber.nj.gov/members).

Other suggested information sources/subscriptions include the US Computer Emergency Readiness Team (US-CERT), as well as vendor-specific information security resources that include vulnerability and security updates for their respective products.

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations.

REFERENCES

The requirements established in the Threat Management policy have been derived from following:

- NIST SP 800-53 Program Management (PM), System and Information Integrity (SI); and
- NIST CSF Identify/Risk Assessment (ID.RA).
VULNERABILITY AND PATCH MANAGEMENT (VU)

PURPOSE
The purpose of the Vulnerability and Patch Management policy is to establish controls and processes to help proactively identify and remediate technical vulnerabilities within information systems, components, and hosted applications.

KEY TERMS
Penetration Test - A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Red Team -- A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Vulnerability – A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Scan - An automated process to proactively identify security weaknesses in a network or individual system.

VU-01: POLICY
Agencies shall implement proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of State information systems and information.

This policy is supported by the following standards and guidelines.

VU-02: VULNERABILITY AND PATCH MANAGEMENT PROGRAM
The State Chief Information Security Officer (CISO) shall:

(a) Develop and implement an enterprise-wide technical Vulnerability and Patch Management Program; and

(b) Utilize a risk-based model for prioritizing remediation of identified vulnerabilities.

Guidelines: Agencies should subscribe to vendor and other security mailing lists to receive notifications of vulnerabilities, patches, and other current security information on the products they employ. The NJCCIC regularly publishes vulnerability alerts as standalone threat intelligence products and within the weekly NJCCIC Bulletin. In accordance with the Threat Management
Policy, agencies are required to register to join the NJCCIC to receive its threat intelligence products.

**VU-03: VULNERABILITY SCANNING**

Agencies shall:

(a) Conduct vulnerability scans for all agency systems and hosted applications prior to their introduction into the production environment;

(b) Conduct a vulnerability scan for any agency system and/or hosted application, after any changes to the asset;

(c) Conduct ongoing vulnerability scans for agency systems and hosted applications, prioritizing the scans based on risk and criticality. The scanning frequency should be no less than monthly on critical systems or when new vulnerabilities potentially affecting the agency information systems or hosted applications are identified and reported;

(d) Perform credentialed scans, where technically feasible. Specifically, information systems must implement privileged access authorization for selected vulnerability scanning activities;

(e) Perform vulnerability scans during hours that will minimize disruption to agency business functions;

(f) Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   
   (1) Enumerating platforms, software flaws, and improper configurations;
   
   (2) Formatting checklists and test procedures; and

   (3) Measuring vulnerability impact;

(g) Analyze vulnerability scan reports and results from security control assessments;

(h) Remediate legitimate vulnerabilities in accordance with an assessment of risk; and

(i) Share information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Guidelines: Security categorization of systems guides the frequency and comprehensiveness of vulnerability scans. Systems containing High Impact information and those critical to an agency’s ability to perform its business functions (“critical systems”) are to receive the highest priority. Agencies are to ensure vulnerability scanning includes all system components and does not overlook less critical components such networked printers, scanners, and copiers. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning. For sensitive systems, for which
providing privileged access to conduct scans is not permitted, a host-based scanning agent should be employed.

**VU-04: VULNERABILITY RANKING**
In accordance with the Information Security Risk Management Program, risks must be:

(a) Ranked; and

(b) Prioritized accordingly for remediation.

Guidelines: The National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system is used as a reference to assist in ranking vulnerabilities. The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

**VU-05: VULNERABILITY REMEDIATION PROCESS**
Agencies are required to use a Plan of Action and Milestones (POA&M), or some other agency-approved method, as a key tool in documenting identified vulnerabilities, their status, and remediation steps.

Guidelines: POA&M, a ticketing-based system, or another formalized method that allows for the tracking of vulnerabilities and their remediation, should be implemented by Agencies.

**VU-06: VULNERABILITY REMEDIATION**
Agencies are required to:

(a) Proactively review systems and applications for vulnerabilities and misconfigurations through:

(1) Utilization of vulnerability assessment tools or methods:
   a. At least monthly; and
   b. After any changes to the asset;

(2) The implementation of a Web Application Firewall (WAF) solution that detects and prevents web-based attacks for public facing web applications;

(b) Review identified vulnerabilities and misconfigurations for applicability and potential impact;

(c) Apply a risk-based approach to prioritize the remediation of vulnerabilities; and

(d) Follow agency change control processes to implement remediation steps.
Guidelines: Public-facing web applications are primary targets for attackers. Poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices.

- Manual or automated vulnerability security assessment tools or methods are used to review and/or test the application for vulnerabilities; and
- Web-application firewalls filter / block nonessential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured.

VU-07: SOFTWARE PATCHING
Agencies are required to ensure that:

(a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
(b) Critical security patches are installed within thirty (30) days of the vendor’s release date; and
(c) Non-critical security patches are installed within ninety (90) days of the vendor’s release date.

Guidelines: Agencies should apply a risk-based approach to prioritize patch installations.

Agencies are required to ensure systems are maintained and updated to manufacturer's specifications. This helps ensure that existing solutions are operating properly throughout their lifecycles.

VU-08: PENETRATION TESTING
The State Chief Information Security Officer shall coordinate authorized external and internal penetration testing with Agency CIOs and CISOs that includes the following:

(a) Is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115);
(b) Testing is to be performed from both inside and outside the network;
(c) Testing to validate any segmentation and scope-reduction controls;
(d) Defines application-layer penetration tests;
(e) Defines network-layer penetration tests to include components that support network functions as well as operating systems;
(f) Reviews threats and vulnerabilities experienced in the last twelve (12) months;
(g) Internal and external testing that occurs at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment);

(h) Vulnerabilities found during penetration testing are corrected, and testing is repeated to verify the corrections; and

(i) Submits penetration results documentation to the State Chief Information Security Officer.

Guidelines: The testing methods must be approved by the State CISO. A standard method for penetration testing includes:

- Pretest analysis based on full knowledge of the target system;
- Pretest identification of potential vulnerabilities based on pretest analysis; and
- Testing designed to determine exploitability of identified vulnerabilities.

If segmentation is used to isolate sensitive enclaves from other networks, penetration tests should be performed at least annually, and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

**VU-09: INDEPENDENT PENETRATION TESTING**

The State CISO and his/her designated representatives are authorized to contract for independent penetration agents or a penetration team to perform penetration testing on systems or system components.

Guidelines: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the systems that are the targets of the penetration testing.

**VU-10: RED TEAM EXERCISES**

Red team exercises:

(a) May be used to improve security awareness and training and to assess levels of security control effectiveness;

(b) Are only authorized to be conducted by the State CISO or individual Agency CISO in coordination with the State CISO, so long as the exercise is limited to assets under the auspices of the CISO’s agency; and

(c) Red team exercises authorized by the State CISO will be done so in conjunction with the Agency CIO(s) and CISO(s) for which systems the exercises will impact.
Guidelines: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises should reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of systems and organizations.

REFERENCES
The requirements established in the Vulnerability and Patch Management policy have been derived from the following:

- NIST SP 800-53 System and Service Acquisition (CA), Program Management (PM), System and Information Integrity (SI), Risk Assessment (RA);
- NIST CSF Identify/Risk Assessment (ID.RA), Protect/Information Protection Policies and Procedures (ID.PR), Detect/Detection Processes (DE.DP), Detect/Security Continuous Monitoring (DE.CM), Respond/Mitigate (RS.MI); and
CONTINUOUS MONITORING (CO)

PURPOSE
The purpose of the Continuous Monitoring Policy is to establish and maintain situational awareness within individual agencies, and across the Executive Branch as a whole, through timely collection and review of security-related event logs.

KEY TERMS
Audit Log - A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

Component - A general term that is used to mean one part of something more complex. Scope Note: For example, a computer system may be a component of an IT service, or an application may be a component of a release unit. Components are co-operating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built. However, the goal of component-based development is to ultimately use as many pre-developed, pretested components as possible.

Event - Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Incident - An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Remote Desktop Access Architecture – A high-level remote access architecture that gives a user the ability to remotely control a particular computer at their agency from an external network. Remote desktop access architecture includes, but is not limited to, systems (local and remote) and software (e.g. Cisco AnyConnect, Citrix, GoToMyPC, Verisign Identity Protection (VIP)) that is used to facilitate and secure the remote session. The specific technologies utilized in a remote desktop access architecture are determined by the New Jersey Office of Information Technology.

Security Information and Event Management (SIEM) - Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
**CO-01: POLICY**

Asset custodians and information system owners shall:

(a) Ensure the information assets under their purview are configured in accordance with the Security Engineering and Architecture Policy and the Configuration Management Policy regarding event logging to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed; and

(b) Review and retain event logs in compliance with all applicable State and Federal laws, regulations, and internal agency and State of New Jersey policies.

This policy is supported by the following standards and guidelines.

**CO-02: CONTINUOUS MONITORING**

Asset custodians and information security personnel shall:

(a) Implement processes to capture, protect, and review security event logs from all system components (network devices, workstations, servers, applications, databases, etc.) to identify and manage suspicious activity within their respective agencies;

(b) Forward their security event logs to the NJCCIC in order to aid in identifying and managing threats to individual agencies, and to correlate events across all agencies that comprise the Executive Branch:

(1) Asset custodians and information security personnel shall collect, review, and forward to the NJCCIC the following:

   a. All security events (e.g. malware detection);

   b. Logs of all system components that store, process, or transmit sensitive data, or that could impact the sensitive data;

   c. Logs of all critical system components;

   d. Logs of all servers and system components that perform security functions. This includes, but is not limited to:

      i. Firewalls;

      ii. Intrusion Detection Systems (IDS);

      iii. Intrusion Prevention Systems (IPS);

      iv. Authentication servers (e.g., Active Directory domain controllers);

   e. Authentication logs for all remote access from external networks (e.g. VPN, Web-based Remote Desktop Application, etc.);

   f. Authentication logs for all publicly accessible web applications that store, process, or transmit sensitive data;
g. Web application logs for all publicly accessible web applications that store, process, or transmit sensitive information including cloud based applications;

h. Mail transfer logs (e.g. logs of emails sent/received); and

i. Web proxy and email content filtering logs.

(c) Review logs of all other system components periodically based on sensitivity and criticality of the system components;

(d) Follow up exceptions and anomalies identified during the review process;

(e) Develop processes for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

   (1) Firewalls;
   (2) IDS/IPS;
   (3) File Integrity Monitoring;
   (4) Anti-malware;
   (5) Physical access controls;
   (6) Logical access controls;
   (7) Audit logging mechanisms; and
   (8) Segmentation controls (if used).

(f) Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

   (1) Restoring security functions;
   (2) Identifying and documenting the duration (date and time start to end) of the security failure;
   (3) Identifying and documenting cause(s) of failure, including root cause, and documenting remediation activities required to address the root cause for the failure;
   (4) Identifying and addressing any security issues that arose during the failure;
   (5) Implementing controls to prevent cause of failure from reoccurring; and
   (6) Resuming monitoring of security controls.

Guidelines: There are certain activities that occur on networks, systems, and applications that need to be logged and reviewed on a continuous basis to identify potential threats to agency information and information systems in order to identify anomalous activity or suspicious events. Conducting reviews of security related events within an individual agency and forwarding the logs of the events to the NJCCIC provides both a compartmentalized view and a holistic view of events across the Executive Branch of New Jersey State Government. These include events such
as successful and failed login activity, data requests, data transfers, changes to configuration files, the addition, deletion, or modification of User-IDs, etc.

Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the State will have gaps in its situational awareness that could lead to system compromise and/or data exfiltration. Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support risk management decisions.

**CO-03: CENTRALIZED EVENT LOG COLLECTION**

Asset custodians shall:

(a) Configure all systems, devices, and applications to implement automated audit trails for all system components and automatically forward security-related event logs to a centralized log collector or Security Incident Event Management (SIEM) solution to allow agency and NJCCIC personnel to audit and reconstruct the events;

(b) Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals;

(c) Allocate adequate storage capacity for centralized log collection systems under their purview;

(d) Restrict access to audit logs stored in the centralized log collection system to individuals with a need to know and in accordance with all applicable State and Federal laws, regulations, contracts, and individual agency policies regarding the information contained in the logs;

(e) Configure auditing/logging to reduce the likelihood that such storage capacity will be unnecessarily exceeded; and

(f) Periodically archive logs when no longer needed for active reviews.

Guidelines: Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the sensitive data environments.

Archiving older logs and retaining them in accordance with applicable records retention strategies helps to ensure sufficient storage capacity is maintained. It is important to carefully plan the configured log levels so that important events are not missed amongst the noise that the excessive event logging produces.

All Production systems are to include logs that contain the date and time, as well as user identification, event type, event success or failure, event origination and the affected data, system component or system resource. For logs of security events to be of value they must contain sufficient detail to identify and correlate security events and incidents. Agencies should
consult with the NJCCIC for assistance in configuring systems to produce the most beneficial log data.

The NJCCIC maintains an enterprise Security Information and Event Management (SIEM) system that provides NJCCIC analysts with the ability to contemporaneously identify suspicious activity and correlate events across all agencies. Similarly, the NJCCIC maintains a centralize log collection system that allows it to correlate and/or reconstruct events that occur over time and to satisfy State and Federal statutory, regulatory, and contractual requirements regarding log retention. Agencies should consult with the NJCCIC regarding forwarding of logs and their review.

**CO-04: CONTENT OF AUDIT RECORDS**

Asset custodians shall configure systems to record at least the following audit trail entries for all system components for each event:

- (a) User account, system account, service or process responsible for initiating the system event;
- (b) Type of event;
- (c) Date and time of event;
- (d) Success or failure indication;
- (e) Origination of event;
- (f) Identity or name of affected data, system component, or resource;
- (g) All successful login and logoff attempts;
- (h) All unsuccessful login and authorization attempts;
- (i) All identification and authentication attempts;
- (j) All actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users);
- (k) All actions, connections and requests performed by privileged functions;
- (l) All changes to logical access control authorities (e.g., rights, permissions);
- (m) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
- (n) The creation, modification and deletion of objects including files, directories and user accounts;
- (o) The creation, modification and deletion of user accounts and group accounts;
- (p) The creation, modification and deletion of user account and group account privileges;
(q) System start-up and shutdown functions;

(r) Modifications to administrator account(s) and administrator group account(s) including:
   1. Escalation of user account privileges commensurate with administrator-equivalent account(s); and
   2. Adding or deleting users from the administrator group account(s);

(s) The enabling or disabling of audit report generation services; and

(t) Command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Guidelines: Audit Systems should record logs in a standardized format such as syslog entries. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

**CO-05: PROTECTION OF AUDIT RECORDS**

Audit records are to be protected and retained in accordance with their sensitivity and all applicable State and Federal laws, regulations, contracts, and State and agency-specific policies.

   (a) Asset custodians are required to implement safeguards to protect the audit records from unauthorized disclosure, alteration, and deletion;

   (b) Audit records shall be restricted to personnel routinely responsible for performing security audit functions; and

   (c) Audit logs are to be retained in accordance with all State and Federal laws, regulations, contracts, and internal agency policies governing their retention.

Guidelines: Audit records from web applications may contain highly sensitive information such as passwords, social security numbers, payment card numbers, etc. For systems, they may contain full text recordings of privileged commands. As such, agencies must implement controls to effectively protect the content of the logs from unauthorized disclosure. The use of file integrity monitoring solutions allows for the detection of unauthorized changes to the contents of audit logs and should be considered as a means for ensuring their integrity. As audit logs may contain information protected by State and Federal laws, regulations, contracts, and individual agency policies, agencies must ensure that individuals with access to audit logs have the required training, skills, and background screening, in accordance with applicable laws.

Agencies should refer to State of New Jersey, Chapter 410, Laws of 1953, *Destruction of Public Records Act*, the *State General Records Retention Schedule*, for more information on retention requirements.
**CO-06: REPORTING**

Asset custodians and asset owners shall ensure information assets are configured to:

(a) Automatically generate reports based on pre-defined criteria and thresholds regarding events of interest (e.g. five (5) consecutive failed login attempts in a given time period or any attempt to access a disabled user account); and

(b) Generate reports that allow asset custodians and information security personnel to review potentially significant issues and/or incidents on the system generating the event.

Upon the detection of an information security incident asset custodians and/or the information security personnel shall report and respond to the incident in accordance with the Incident Response Policy contained herein.

Guidelines: Event logging limits identification of anomalous or suspicious activity to only the system for which the log is generated. Reporting allows for the compilation of events across multiple systems to provide a more complete view of related events.

**CO-07: CLOCK SYNCHRONIZATION**

Asset custodians shall configure all systems and applications to use the Network Time Protocol (NTP) and the NJOIT’s approved time sources to ensure clocks are synchronized and log file time stamps are accurate.

Guidelines: Asset custodians may refer to the Security Engineering and Architecture Policy and the Configuration Management Policy included in this manual for more information.

Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization. To ensure time is synchronized across all systems on the GSN agencies should use NJOIT’s time servers.

**REFERENCES**

The requirements established in the Continuous Monitoring Policy have been derived from following:

- NIST SP 800-53 Audit and Accountability (AU), System and Information Integrity (SI); and
- NIST CSF Protect/Protective Technologies (PR.PT), Detect/Continuous Monitoring (DE.CM), Detect/Detection Processes (DE.DP).
PURPOSE
The purpose of this policy is to establish the minimum requirements necessary to ensure that system and application software programs developed by State of New Jersey Executive Branch Departments and Agencies or external entities (vendors and/or contractors) perform as intended to maintain information confidentiality, integrity, and availability.

KEY TERMS
Software Development Life Cycle (SDLC) – The scope of activities associated with the development of a software application that includes planning, analysis, design, testing, and implementation. The acronym, SDLC is interchangeably used to refer to System Development Life Cycle which includes the same scope of activities of a Software Development Life Cycle.

Major Applications and Systems – a major application or system is described as any system or application that includes one or more of the following characteristics:

(a) Includes users in more than one agency;

(b) Costs more than $100,000, to develop and implement (cost includes hardware, software, and contract personnel);

(c) Any public facing web application; and/or

(d) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

SD-01: POLICY
Agencies shall implement the principles of “least privilege” and “least functionality” in the development and implementation of application software. Appropriate security measures based on identified risks, security categorization, legal and regulatory requirements for data protection, are to be incorporated into all phases of Software Development Life Cycle.

This policy is supported by the following standards and guidelines.

SD-02: SECURE DEVELOPMENT
Agencies are required to ensure that internal and external developers:

(a) Develop software applications in accordance with industry-recognized leading practices;

(b) Incorporate cybersecurity throughout the software development lifecycle;

(c) Conduct code reviews prior to release to production in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:
1. Code changes must be reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices;
2. Code reviews must ensure code is developed according to secure coding guidelines;
3. Appropriate corrections must be implemented prior to release; and
4. Code-review results must be reviewed and approved by management prior to release.

(d) Remove custom application accounts, User-IDs, and passwords, both within the code and within any externally leveraged authentication sources before applications are introduced into the production environment; and

Guidelines: Secure development guidelines are based on the Open Web Application Security Project (OWASP) guide.

**SD-03: SECURE CODING**

Agency CIOs and CISOs along with their designees are required to address common coding vulnerabilities in the software development process by ensuring the following:

(a) For in-house developed applications, developers must ensure that development artifacts (e.g., sample data and scripts, unused libraries, components, debug code, or tools) are not included in the deployed software, or accessible in the production environment;

(b) At least annually, developers are properly trained in current, secure coding techniques, including:
   1. How to avoid common coding vulnerabilities;
   2. Understanding how sensitive data is handled in memory; and

(c) Applications are developed based on secure coding guidelines.

Guidelines: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.

**SD-04: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS**

Agencies shall:

(a) Maintain and manage baseline configurations for development and test environments separately from its production baseline configurations;

(b) Separate production and non-production environments to prevent unauthorized access or changes to production applications, configurations, and systems; and

(c) Prevent developers from having unmonitored access to production environments.
Guidelines: Separation of the environments may include firewalls, authentication sources, and clear separation of duties for personnel accessing these environments as part of their job duties.

Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow agencies to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. This standard requires separate configurations but not necessarily separate physical environments.

**SD-05: INFORMATION INPUT RESTRICTIONS**

For custom-developed applications and web pages, agencies are required to enforce rules to require inputs to be prescreened to prevent the inputs from being unintentionally interpreted as commands.

Guidelines: Input restrictions are important to prevent against common hacking techniques that take advantage of poor software development principles (e.g., SQL injection and buffer overflow attacks).

**SD-06: INPUT DATA VALIDATION**

On custom-developed applications and web pages, agencies shall ensure that rules for checking the valid syntax and semantics of system inputs are in place to verify that inputs match specified definitions for format and content. System inputs include, but are not limited to:

- (a) Character set;
- (b) Length;
- (c) Numerical range; and
- (d) Acceptable values.

Guidelines: Checking the valid syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

**SD-07: ERROR HANDLING**

Agencies are required to examine the structure and content of error messages to ensure error messages do not disclose sensitive information or add risk to the security of the system or information.

Guidelines: Asset custodians are required to carefully consider the structure/content of error messages. Sensitive information may include, for example, erroneous login attempts with
passwords entered by mistake as the username, mission or business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers.

SD-08: SECURITY TESTING THROUGHOUT DEVELOPMENT

Software developers and system integrators are required to:

(a) Follow change control processes and procedures for all changes to system components that affect the application’s production network;

(b) Supervise, monitor, and document the activity of outsourced system development;

(c) For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats;

(d) Perform static and dynamic code analysis of custom code prior to release to production, in order to identify any potential coding vulnerability;

(e) Remove test data and accounts, both within the code and within any externally leveraged authentication sources before production systems are elevated to production; and

(f) Ensure security functionality testing is conducted, documented, and reviewed prior to implementation.

Guidelines: Agencies should follow a defined change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services. The change control processes should include the following:

- Separate development/test and production environments;
- Separation of duties between development/test and production environments;
- Production data (live data) are not used for testing or development; and
- Removal of test data and accounts before production systems become active.

Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static analysis can identify defects and provide clear remediation guidance to enable developers to fix such defects.

Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs.
SD-09: USE OF LIVE DATA
Production data shall not be replicated or used in non-production environments:

(a) Any use of production data in non-production environments requires explicit, documented approval from the agency CISO, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements; and

(b) The use of Sensitive Personally Identifiable Information (SPII) is prohibited from use in testing or development environments.

Guidelines: The use of live data in preproduction environments can result in significant risk to agencies. Agencies can minimize such risk by using test, or dummy data during the development and testing of information systems, information system components, and information system services.

SD-10: ACCESS TO PROGRAM SOURCE CODE
Access to agency developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege, based on job function.

SD-11: TRAINING
Agencies shall provide and require developers and asset custodians with role-based training specific to the security requirements of the responsibilities and duties.

Guidelines: Role-based training may include secure coding training, systems administration training, security testing training, etc. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training.

REFERENCES
The requirements established in the Security in Software Development policy have been derived from following references:

- NIST SP 800-53: Planning (PL); Project Management (PM); Systems and Services Acquisition (SA); Security Assessment and Authorization (CA); System and Information Integrity (SI); System and Communication Protection (SC); Security Awareness Training (AT); and

- NIST CSF: Protect/Data Security (PR.DS); Protect/Awareness and Training (PR.AT).
SECURITY FOR PUBLICLY-ACCESSIBLE WEBSITES AND SERVICES (WS)

PURPOSE
Publicly-accessible State websites and services are essential resources through which the public receives information from, and interacts with, State government agencies. These websites and services help the public apply for benefits, search for jobs, comply with State rules and regulations, obtain authoritative information, and much more. As such, it is imperative that all New Jersey State Government websites and services provide security and privacy assurances to those who use them.

The purpose of this policy is to address the risks associated with State Government websites and services, and to provide agencies with guidance on the minimum controls necessary to assure authenticity for State Government websites and services and to prevent a loss of confidentiality, integrity, privacy, and availability.

KEY TERMS
HTTPS (HTTP Secure) - is an adaptation of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security. HTTPS is also commonly referred to as HTTP over TLS or HTTP over SSL.

Publicly-Accessible Websites and Services – consist of online resources and services available over HTTP or HTTPS over the public internet that are maintained in whole or in part by NJ State Government and operated by an agency, contractor, or other organization on behalf of the agency. They present State government information or provide services to the public or a specific user group and support the performance of an agency’s mission. This definition includes all web interactions, whether a visitor is logged-in or anonymous.

WS-01: POLICY
Agencies shall implement the principles of “least privilege” and “least functionality” in managing New Jersey State Government websites and Internet-accessible services and ensure appropriate security and privacy controls are implemented to satisfy applicable statutory, regulatory and contractual requirements.

This policy is supported by the following standards and guidelines.

WS-02: HTTPS-ONLY
All publicly accessible State of New Jersey Executive Branch Government websites and web services shall provide secure and private connections through the use of an HTTPS connection.
(a) Newly developed websites and services at all New Jersey State agency domains or subdomains must adhere to this policy upon launch; and

(b) For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), or where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic, should receive priority and migrate as soon as possible.

Guidelines: The unencrypted HTTP protocol does not protect data from interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data. Unencrypted HTTP connections create a privacy vulnerability and expose potentially sensitive information about users of unencrypted State websites and services. The requirement to use HTTPS-Only for State government websites will eliminate inconsistent, subjective determinations across agencies regarding which content or browsing activity is sensitive in nature and create a stronger privacy standard enterprise-wide. As agencies implement HTTPS-Only websites they will need to consider implementing HTTP Strict Transport Security (HSTS) preload to ensure browsers always use an https:// connection.

Considerations for migrating to HTTPS:

- **Site Performance:** While encryption adds some computational overhead, modern software and hardware can handle this overhead without substantial adverse impact on server performance or latency. Websites with content delivery networks or server software that support the SPDY or HTTP/2 protocols, which require HTTPS in some major browsers, may find their site performance substantially improved as a result of migrating to HTTPS;

- **Server Name Indication:** The Server Name Indication extension to TLS allows for more efficient use of IP addresses when serving multiple domains. However, these technologies are not supported by some legacy clients. Web service owners should evaluate the feasibility of using this technology to improve performance and efficiency;

- **Mixed Content:** Websites served over HTTPS need to ensure that all external resources (images, scripts, fonts, iframes, etc.) are also loaded over a secure connection. Modern browsers will refuse to load many insecure resources referenced from within a secure website. When migrating existing websites, this can involve a combination of automated and manual effort to update, replace, or remove references to insecure resources. For some websites, this can be the most time-consuming aspect of the migration process;

- **APIs and Services:** Web services that serve primarily non-browser clients, such as web APIs, may require a more gradual and hands-on migration strategy, as not all clients can be expected to be configured for HTTPS connections or to successfully follow redirects; and

- **Planning for Change:** Protocols and web standards improve regularly, and security vulnerabilities can emerge that require prompt attention. State websites and services
should deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices (including forward secrecy) protocol versions, and other configuration elements.

- **Strict Transport Security**: Websites and services available over HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward. This reduces insecure redirects and protects users against attacks that attempt to downgrade connections to plain HTTP. Once HSTS is in place, domains can be submitted to a “preload list” used by all major browsers to ensure the HSTS policy is in effect at all times.

**WS-03: USE OF DEMILITARIZED ZONES (DMZ)**

For all publicly facing Internet accessible technologies hosted within the Garden State Network, the NJOIT shall implement and configure a Demilitarized Zone (DMZ) in order to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

Guidelines: A DMZ functions as an isolated network positioned between the Internet and internal agency systems. Traffic from the Internet is to be restricted to only IP addresses in the DMZ, and only connections from those IP addresses should be allowed to pass through the firewall(s) that protect internal agency networks. For websites, typically a web server will be placed in the DMZ but all sensitive information served to the public is located on an internal network protected from external network access by a firewall or other means.

**WS-04: WEB APPLICATION FIREWALL (WAF)**

As part of the State’s defense in-depth approach to information security all publicly-facing websites shall be protected by Web Application Firewalls (WAFs) that inspect all traffic flowing to the website for common web application attacks, including but not limited to:

(a) Cross-site scripting;
(b) SQL injection;
(c) Session hijacking;
(d) Buffer overflows;
(e) Command injection; and
(f) Directory traversal attacks.

Guidelines: Website and web application vulnerabilities account for one of the largest portions of attack vectors by malicious actors. To help prevent the exploit of website and web application vulnerabilities, web application firewalls, with the capability to inspect both unencrypted and encrypted traffic directed at State websites, should be deployed.
WS-05: ACCESS CONTROLS FOR PUBLICLY-FACING WEB APPLICATIONS

Agencies shall protect public-facing web applications requiring authentication by deploying reasonably-expected security controls, including but not limited to the following requirements:

(a) Passwords having the following attributes:
   (1) Required to be at least eight (8) characters in length;
   (2) Not contain the user’s account name or parts of the user’s full name that exceed two consecutive characters;
   (3) Required to contain characters from each of the following four (4) categories:
       a. English uppercase characters (A through Z);
       b. English lowercase characters (a through z);
       c. Base 10 digits (0 through 9); and
       d. Non-alphanumeric characters (for example: !, $, #, >, %).

(b) For publicly accessible web applications that provide the general public with access to Sensitive Personally Identifiable Information (SPII), agencies shall offer users the option of using Multi-Factor Authentication for added protection, as technically feasible;

(c) For publicly-accessible web applications that provide agency personnel with access to agency systems containing sensitive information, multi-factor authenticate shall be required in accordance with the Identity and Authentication Policy;

(d) Default session timeout after a period of fifteen (15) minutes of inactivity; and

(e) Account lockout after five (5) failed login attempts.

Guidelines: Agency websites often provide the general public with access to SPII (e.g. pay stubs, retirement, and health benefits information, etc.) which if accessed without authorization could result in significant harm to individuals. The option to use multi-factor authentication to access an individual’s SPII information provides an added layer of protection for the individual.

WS-06: PRIVACY

State Government agencies necessarily create, collect, use, process, store, maintain, disseminate, disclose, and dispose of personally identifiable information (PII) to carry out missions mandated by State and Federal statutes. For all publicly accessible web sites and web applications, agencies shall adhere to the requirements as documented in the Privacy Policy included in this Manual, The State of New Jersey Technology Circular, On-Line Privacy Policy, 13-09-OIT, and all applicable State and Federal laws regarding privacy.

Guidelines: The review of privacy risks should begin at the earliest planning and development stages of agency actions and policies that involve PII and should continue throughout the life cycle of the information. Agencies must be transparent about policies and practices with respect to PII and must provide clear and accessible notice regarding the creation, collection,
use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. This includes maintaining an up-to-date Privacy Program Page on an agency’s principal website, posting plain language privacy policies on an agency’s websites, mobile applications, and other digital services, providing Privacy Act statements where required by the Privacy Act of 1974, and providing privacy notices for online collections of information where feasible.

A privacy notice must be provided, whenever feasible, where a Privacy Act statement is not required but members of the public could nonetheless provide PII to the agency using an online interface. The privacy notice should include a brief description of the agency’s practices with respect to the PII that the agency is collecting, maintaining, using, or disseminating.

**WS-07: APPROVED DOMAINS**

Agencies shall follow the Policies and Procedures contained in the *State of New Jersey Technology circular, Internet and Statewide Intranet Presence for New Jersey State Government Policy, 14-11-NJOIT* regarding the use of approved domains and other website requirements.

Guidelines: Currently, the primary way users quickly determine if they are on an official New Jersey State Government website is to look for the nj.gov or state.nj.us designation as part of the domain name. The nj.gov and state.nj.us domains are widely viewed as zones of increased trust, where the public can confidently access government information and services in a secure environment knowing that the site is legitimate and authoritative. Requiring State websites to be part of the nj.gov or state.nj.us domain instills greater confidence in agency public websites and digital services.

**WS-08: PUBLICLY ACCESSIBLE CONTENT**

Agencies shall:

(a) Designate individuals authorized to post information onto the agency’s publicly accessible information system;

(b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

(c) Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

(d) Review the content on the publicly accessible information system for nonpublic information and removes such information, if discovered.

**REFERENCES**

The requirements established in the Security for Publicly-Accessible Websites and Services have been derived from following:

- NIST SP 800-53 Secure Communications (SC), Systems Integrity (SI)
• NIST CSF Protect/Access Control (PR-AC). Protect/Protective Technologies (PR-PT)
PROJECT AND RESOURCE MANAGEMENT (PM)

PURPOSE
The purpose of the Project and Resource Management Policy is to ensure that controls necessary to appropriately manage risks are accounted for and implemented throughout the System Development Life Cycle (SDLC).

KEY TERMS
Major Applications and Systems – a major application or system is defined as any system or application that includes one or more of the following characteristics:

(a) Includes users in more than one agency;
(b) Costs more than $100,000 to develop and implement (cost includes hardware, software, and contract personnel);
(c) Any public facing web application; and/or
(d) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

System Development Life Cycle (SDLC) - The scope of activities associated with an information system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

PM-01: POLICY
Agencies shall implement and maintain appropriate security controls through the life cycle of all information assets, including all information systems and services under their purview.

This policy is supported by the following standards and guidelines.

PM-02: ALLOCATION OF RESOURCES
The Agency Chief Information Security Officer (CISO) and his/her designated representatives are responsible for managing and providing oversight for the cybersecurity-related aspects of the planning and service / tool selection process. The CISO is required to:

(a) Include information security requirements in business process planning; and
(b) Allocate resources required to protect agency systems and information, as part of its capital planning process.

Guidelines: To apply needed security controls within the System Development Life Cycle (SDLC) (including the acquisition process), requires a basic understanding of cybersecurity, threats, vulnerabilities, and risk to critical missions/business functions. Security engineering principles cannot be properly applied if individuals that design, code, and test systems and system...
components (including information technology products that are used to build those systems/components) do not understand security. Therefore, agencies should include qualified information security personnel in SDLC activities to ensure that security requirements are incorporated into organizational systems. The OHSP Division of Cybersecurity may be called upon by agencies to assist in the development of information security requirements.

**PM-03: SECURITY REQUIREMENTS DEFINITION**

Agencies are required to:

(a) Define and document the security requirements necessary to adequately protect critical system components; and

(b) Identify and remediate vulnerabilities throughout the SDLC.

**PM-04: SECURITY IN PROJECT MANAGEMENT**

A formal cybersecurity risk analysis must be performed on all significant development and/or acquisitions, prior to information systems being placed into production:

(a) New information systems and applications must be appropriately tested for security functionality prior to being placed in production; and

(b) Agency asset custodians and data/process owners are required to perform a gap analysis, at least once per year, to determine any deviations from their systems’ current state of compliance and that which is required.

Guidelines: Tests for security functionality include vulnerability scans and remediation of all vulnerabilities, penetration tests, and other tests to ensure the requisite security controls have been implemented.

**PM-05: SYSTEM SECURITY PLAN**

For all major applications in development, or undergoing significant changes, a System Security Plan shall be submitted to the OHSP Division of Cybersecurity to ensure the appropriate security requirements are defined and implemented based on identified risks, information security categorization, legal and regulatory requirements for data protection, and adherence to Executive Branch information security policies and standards. The SSP shall also be submitted to the New Jersey Office of Information Technology (NJOIT) to ensure all new projects align with the enterprise information technology architecture strategy.

Guidelines: The System Security Plan is to be submitted along with a Privacy Impact Analysis as part of the NJOIT System Architecture Review process.

**PM-06: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)**

For all major system and application development and/or acquisitions, agencies are required to:

(a) Manage systems using a System Development Life Cycle (SDLC) that includes information security considerations; and
(b) Define and document information security roles and responsibilities throughout the SDLC.

Guidelines: The level of detail required in security-related documentation is based on the security categorization of the system and its information. Adhering to an SDLC ensures that systems and software will be adequately documented and tested before being used for critical business processes, while also mitigating the risks associated with threats to confidentiality, integrity, and availability.

REFERENCES
The requirements established in the Project and Resource Management policy have been derived from the following references:

- NIST SP 800-53: Planning (PL), Project Management (PM), Systems and Services Acquisition (SA), Security Assessment and Authorization (CA); and
CAPACITY AND PERFORMANCE PLANNING (CA)

PURPOSE
The purpose of the Capacity and Performance Planning Policy is to ensure that all current and future capacity and performance aspects of the Information Technology (IT) infrastructure are provided to meet business requirements and prevent avoidable interruptions caused by capacity and performance limitations.

KEY TERMS
None. See Glossary in Appendix B for complete listing of terms.

CA-01: POLICY
Agencies shall protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technology and supporting infrastructure.

This policy is supported by the following standards and guidelines.

CA-02: CAPACITY MANAGEMENT
Agencies are required to allocate sufficient processing and storage capacity to reduce the likelihood of exceeding capacity that could negatively impact functionality:

(a) The availability, quality, and adequate capacity of compute, storage, memory and network resources shall be planned, prepared, and measured to deliver the required system performance by legal, statutory, and regulatory compliance obligations; and

(b) Projections of future capacity requirements shall be made to mitigate the risk of system overload.

Guidelines: Agencies must consider the types of processing to be performed and the storage requirements when planning systems. Allocating sufficient storage and performance capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of system capability.

CA-03: RESOURCE PRIORITY
Agency asset custodians and data/process owners are required to prioritize resources to prevent or limit Denial of Service (DoS) attack effectiveness.

Guidelines: Priority protection helps prevent lower-priority processes from delaying or interfering with the system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users/roles. Asset custodians should
also refer to the Network Security Policy that includes DoS requirements to protect network-based denial of service attacks.

**REFERENCES**

The requirements established in the Capacity and Performance Planning Policy have been derived from the following:

- NIST SP 800-53 System and Communications Protection (SC); and
- NIST CSF Protect/Data Security (PR.DS).
PURPOSE
The purpose of the Third Party Management Policy is to ensure that appropriate processes and security measures are implemented to manage risks associated with third parties at acceptable levels.

KEY TERMS
System Interconnection: is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections include connections that are permanent in nature, connections that are established by automated scripts at prescribed intervals, and/or connections which utilize web and SOA services. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser.

External Connections:
System or IP addressable end points that are not under the direct control of the Executive Branch of New Jersey State Government, systems that have IP addressing not in the Executive Branch’s addressing scheme (routable and non-routable), or systems that have an authorizing official who is not an Executive Branch employee.

Extranet: is a private network that uses Internet technology and the public telecommunication system in order to securely share part of a business’s information or operations with suppliers, vendors, partners, customers, or other businesses. In the case of the State of New Jersey, the Extranet can include firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages through the use of a SSL tunnel, and the use of virtual private networks (VPNs) that tunnel through the public network.

Sponsoring Agency: The Agency that has acquired the services of a third party or otherwise responsible for granting physical and/or logical access to facilities, information, and/or information systems to entities external to the Agency, to include but not limited to, those defined as a third party.

Third Party: Any entity, organization, or computing environment that is not an Agency or computing environment governed by the policies and standards contained in the Executive Branch of New Jersey State Government Statewide Information Security Manual. Third parties include, but are not limited to: municipal, county, and federal government organizations,
academic institutions, private businesses, non-profit organizations, information technology equipment, software, and service suppliers, vendors, business partners, affiliates, and others.

**Third Party Interconnection:** is a connection between an Agency’s internal networks and/or systems with:

(i) A system or IP addressable end point that is not under the direct control of an Agency governed by the policies and standards of the Executive Branch of New Jersey State Government Statewide Information Security Manual;
(ii) Systems that have IP addressing not in the State addressing scheme (routable and non-routable); or
(iii) Systems that have an authorizing official who is not a State of New Jersey employee.

**TP-01: POLICY**

Agencies shall implement appropriate processes and security measures necessary to manage information security risks associated with third parties at acceptable levels.

This policy is supported by the following standards and guidelines.

**TP-02: THIRD PARTY RISK ASSESSMENTS**

Agencies shall conduct due diligence risk assessments of third parties prior to establishing business relationships with third party entities that:

(a) Provide information technology equipment, software, and/or services to the Agency;
(b) Have access to internal Agency systems, network, or sensitive information; and/or
(c) Provide information technology and communications services to the Agency.

Guidelines: As part of the risk assessment process, agencies must identify, assess, and prioritize the management of risks at acceptable levels based on the security categorization of the information, information system, components, and/or services the third party provides and/or has access to. Due diligence risk assessments of third parties include, but are not limited to: direct observation (e.g. onsite visits) of the third party, reviews of the third-party’s information security policies and standards, reviews of independent audit reports of the third party, relevant certifications, open source searches, and reference checks.

**TP-03: CONTRACT REQUIREMENTS**

Agencies are required to follow all applicable State and federal laws, and all applicable NJOIT and Department of Treasury, Division of Purchase and Property (DPP) requirements in the procurement and acquisition of IT equipment, software, and services. Agencies are required to maintain written and executed agreements with third parties to ensure:

(a) Confidentiality and Non-Disclosure Agreements (NDA) are agreed to and executed in order to protect against the disclosure of confidential information by the third party and/or the sponsoring agency;
(b) Third-party providers of information technology services and/or connected partners are subject to the same security policies and procedures as the supported agency and shall conform to the same security controls and documentation requirements as they apply to the Agency’s internal systems;

(c) Any outsourcing agreements contain security provisions specifically tailored to the particular outsourcing initiative;

(d) Appropriate management, operational and technical control safeguards are in place to facilitate the confidentiality, integrity, availability, and privacy of the agency’s sensitive information the third party generates, accesses, receives, stores, processes, or transmits; and

(e) Third parties acknowledge in writing that they are responsible for the security of the sensitive information that the third party possesses or otherwise stores, processes, or transmits on behalf of the Agency.

Guidelines: All contracts associated with third parties having access to an Agency’s sensitive information should specify:

- All sensitive information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- The third party must be compliant with and maintain compliance with the protective conditions outlined in the contract;
- Any violation of the protective conditions outlined in the contract amounts to a material breach of contract and entitles the Agency to terminate the contract without penalty;
- The third party is liable to protect all sensitive information it stores and/or accesses;
- In the event of a security breach, due to its actions or inactions, the third party shall bear all responsibility and expenses associated with the response to the security breach;
- The third party must return or destroy all sensitive information received from the agency, upon completion of the contract;
- Auditing of the third party’s security posture and compliance is authorized at any time; and
- The contract’s protective requirements shall survive any termination agreement.

TP-04: THIRD-PARTY INTERCONNECTIONS

State agencies regularly share information with, and provide access to, internal information and information systems to third parties in the normal course of conducting State business. This includes the establishment of third-party interconnections with:

(a) A system or IP addressable end point that is not under the direct control of an Agency governed by the policies and standards of the Executive Branch of New Jersey State Government Statewide Information Security Manual;
(b) Systems that have IP addressing not in the State addressing scheme (routable and non-routable); and/or

(c) Systems that have an authorizing official who is not a State of New Jersey employee.

In accordance with the provisions of the Network Security Policy, the NJOIT shall be responsible for the implementation of third-party interconnections to internal agency systems and networks.

(d) All third-party interconnections shall be made in accordance with the procedures and requirements documented in State of New Jersey IT Circular, 169-00-01 – Business Entity, IT Services and/or Extranet, No. 09-11-P1-NJOIT regarding Extranets;

(e) Third-party interconnections require a signed contract and/or a system interconnection security agreement;

(f) At a minimum, the following details shall be required for all third-party interconnections:

   (1) Description of the business purpose of the connection;

   (2) Updates to agency logical and physical topology diagrams to account for the connection (or a supplementary diagram);

   (3) Allowed protocols;

   (4) Allowed network addresses or address ranges;

   (5) Allowed TCP/UDP ports if applicable;

   (6) Allowed data types; and

   (7) Authorized users (with specific names or user groups);

(g) The third party shall be required to provide contact information, including emergency contact information for off-hours requests and information security incidents;

(h) Third-party interconnections shall be enabled in accordance with the principle of least privilege;

(i) Connectivity to an agency local area network (LAN) or Wide-Area Network (WAN) by a third-party owned or supplied computer system constitutes full network access, and without compensating controls, shall be disallowed by default. Alternatives to connecting to an agency LAN or WAN include:

   (1) Provisioning an agency-owned workstation for use by third party staff who require access to agency systems; and/or

   (2) Provisioning a guest network for third party Internet access from an agency facility;

(j) All third-party interconnections to internal agency networks or systems shall require review and authorization by the sponsoring Agency’s CISO;

(k) All third-party interconnections to internal agency networks or systems shall require review and authorization by the NJOHSP Division of Cybersecurity; and
Third-party interconnections shall not be authorized until security monitoring of that connection has been enabled in accordance with the requirements documented in the Continuous Monitoring Policy.

Guidelines: All third-party interconnections should be planned so that all risks are managed and contractual requirements are established prior to their implementation. The concept of least privilege is to be applied for all individual information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required business functions. Continuous monitoring allows the sponsoring Agency to maintain on-going situational awareness of the functions, ports, protocols, and services that are being employed. Additional information on best practices for implementing third party interconnections can be found in NIST Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems.

TP-05: THIRD PARTY MANAGEMENT
Agencies shall ensure third parties demonstrate compliance with information security and confidentiality, access control, and service delivery level agreements specified in contracts. Agencies are required to:

(a) Maintain a list, and all relevant details, including Service Level Agreements (SLA) regarding third parties:
   (1) That have access to internal agency networks, systems, and information;
   (2) That host agency information systems, applications, and information; and/or
   (3) That supply the Agency with information technology equipment, software, and services;

(b) Maintain written agreements that include acknowledgment for the respective roles and responsibilities as they pertain to the security of Agency information systems and information the third parties possess or otherwise store, process or transmit on behalf of the Agency;

(c) Provide third parties with a copy of the Statewide Information Security Manual as well as any applicable Agency security policies and procedures;

(d) Require that providers of external systems employ appropriate security controls in accordance with the policy and standards requirements in this Manual and all applicable laws and regulatory requirements;

(e) Maintain information about which security requirements are managed by each service provider, and which are managed by the Agency;

(f) Periodically review relationships with third parties to ensure compliance with contractual requirements, security requirements, and business need; and
(g) Continuously monitor access to agency information systems and information by authorized third parties, as well as systems and information outsourced or otherwise provided for or maintained by authorized third parties.

Guidelines: Agencies should periodically review the list of third parties that have access to the Agency’s sensitive information or information systems, provide equipment, software, or services to determine if the business relationship is necessary, and to verify that the third party continues to abide by the terms of the contract.

**TP-06: THIRD PARTY PERSONNEL SECURITY**

Agencies shall implement processes and controls necessary to ensure third-party personnel access is granted only to individuals who:

(a) Have a valid access authorization;

(b) Satisfy associated personnel security criteria (e.g. screening and criminal background checks, as applicable);

(c) Have read, understand, and signed a Non-Disclosure Agreement (NDA) and/or Confidentiality Agreement;

(d) Have successfully completed the information security awareness training in accordance with the Security Awareness and Training Policy;

(e) Have been provided with access to policies and standards included in this Manual, as well as any applicable agency information security policies; and

(f) Have read, understand, and signed an acknowledgment that he or she understands and will abide by the Rules of Behavior - Acceptable Use of State Information Assets Policy.

**TP-07: SUPPLY CHAIN PROTECTION**

Agencies shall:

(a) Work in conjunction with the NJOHSP Division of Cybersecurity, NJOIT, and the Department of Treasury Division of Purchase and Property to conduct due care reviews of suppliers prior to entering into contractual agreements to acquire system hardware, software, firmware, or services;

(b) Employ tailored acquisition strategies, contract tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;

(c) Employ security safeguards to limit harm from potential adversaries identifying and targeting the organizational supply chain; and

(d) Employ security safeguards to validate those information systems or system components received are genuine and have not been altered.
Guidelines: Supply chain risk is part of advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example:

- Avoiding the purchase of custom configurations to reduce the risk of acquiring systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations;
- Employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; and
- Employing approved vendor lists with standing reputations in industry.

**TP-08: TRUSTWORTHINESS**

The Agency CISO and his/her designated representatives are responsible for developing and implementing processes to facilitate the trustworthiness of systems, system components, or system services supporting the Agency’s critical missions/business functions.

Guidelines: Agencies should consider product evaluations conducted through the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (NIAP CCEVS) when purchasing Commercial-Off-the-Shelf (COTS) IT products. NIAP CCEVS oversees evaluations of commercial IT products for use in National Security Systems. NIAP evaluations are conducted by NVLAP-accredited commercial testing labs, called Common Criteria Test Labs (CCTLs). A product vendor chooses an approved lab to complete the product evaluation against applicable Protection Profile(s). A Protection Profile is an implementation-independent set of security requirements and test activities for a particular technology that enables achievable, repeatable, and testable evaluations.

Similarly, the Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

**REFERENCES**

The requirements established in the Third Party Management Policy have been derived from the following:

- NIST SP 800-53 System and Service Acquisition (SA);
- NIST CSF Identify/Supply Chain Risk Management (ID.SC), Identify/Business Environment (ID.BE), Identify/Governance (ID.GV).
SECURITY ASSESSMENT AND AUTHORIZATION (SA)

PURPOSE
The purpose of the Security Assessment and Authorization Policy is to ensure that the security controls for all major systems and applications and general support systems are assessed, and risks are managed to acceptable levels, prior to deployment to operational status.

KEY TERMS
External Connections - System or IP addressable end points that are not under the direct control of the Executive Branch of New Jersey State Government, systems that have IP addressing not in the Executive Branch’s addressing scheme (routable and non-routable), or systems that have an authorizing official who is not an Executive Branch employee.

General Support System - a general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- Local area network (including workstations, printers, and other assets that support an agency office or facility);
- Backbone network (e.g. agency-wide and/or statewide (GSN));
- Agency data processing center including its operating system and utilities (e.g. server room); and/or
- Shared information processing service facility (e.g. data center).

Major Applications and Systems – a major application or system is described as any system or application that includes one or more of the following characteristics:

- Includes users in more than one agency;
- Costs more than $100,000 to develop and implement (cost includes hardware, software, and contract personnel);
- Any public facing web application; and/or
- Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place, or planned, for meeting those requirements.
SA-01: POLICY
All new major applications, general support systems, and external connections, as well as any major applications, general support systems, and external connections in development, or undergoing substantive changes, are required to undergo a security assessment by the NJOHSP Division of Cybersecurity to ensure adequate security controls are implemented, and risks managed to acceptable levels, prior to placement into an operational status.

This policy is supported by the following standards and guidelines.

SA-02: SECURITY CATEGORIZATION
In accordance with the Security Categorization Policy, Information System Owners in conjunction with Information Owners, Agency CISOs and Privacy Officers are required to categorize assets and information according to their sensitivity and criticality. Protection mechanisms shall be implemented commensurate with the impact should there be a loss confidentiality, integrity, and/or availability of the asset or information.

Agencies shall use the following impact levels when assigning security categorizations.

**Low Impact**: The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations; or the State of New Jersey. i.e.

1. Causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
2. Results in minor damage to organizational assets;
3. Results in minor financial loss; or
4. Results in minor harm to individuals.

**Moderate**: The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations; or the State of New Jersey. i.e.

1. Causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in significant damage to agency assets;
3. Results in significant financial loss; or
4. Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
**High Impact:** The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations; or the State of New Jersey i.e.

1. Causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in major damage to organizational assets;
3. Results in major financial loss; or
4. Results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).

**SA-03: PRIVACY IMPACT ASSESSMENT**

Agencies shall implement a privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

(a) Agencies shall conduct Privacy Impact Assessments (PIA) for new information systems, systems under development, systems undergoing changes or upgrades, or other activities that pose a privacy risk;

(b) Agencies shall ensure a Privacy Impact Assessment is conducted prior to any new collection of PII, or upon significant changes in the architecture, information flow, or use of PII within existing systems; and

(c) The Privacy Impact Assessment shall be documented and used by the agency to identify and implement appropriate controls necessary to protect PII in accordance with all applicable State and Federal laws, regulations, and internal agency policies.

Agencies shall submit a completed PIA Form to the State Chief Information Security Officer, or his/her designee, as part of the NJOIT System Architecture Review (SAR) process. The initial draft of The PIA Form is required to be submitted at the time the Logical SAR document is submitted. The PIA Form can be found on the NJCCIC Intranet site.

**SA-04: SYSTEM SECURITY PLAN**

For any new major applications, general support systems, and external connections, as well as any major applications, general support systems, and external connections in development, or undergoing substantive changes, a System Security Plan (SSP) shall be submitted to the OHSP Division of Cybersecurity to ensure the appropriate security requirements are defined and implemented based on: identified risks, security categorization, legal and regulatory requirements for data protection, and adherence to information security policies and standards contained in this Manual, as well as all agency-specific information security policies and standards. The SSP shall also be submitted to the New Jersey Office of Information Technology (NJOIT) to ensure all new projects align with the enterprise information technology architecture strategy.
The System Security Plan review augments the NJOIT System Architecture Review (SAR) process. The initial draft of the SSP is required to be submitted at the time the Logical SAR document is submitted. The SSP Form can be found on the NJCCIC Intranet site.

Guidelines: Examples of when SSPs are required for substantive changes include, but are not limited to: the migration to new operating systems and new operating configuration standards (e.g. Windows Server 2008 to Windows Server 2016), the migration or implementation of new hardware or equipment implementations (e.g. firewalls, switches, servers, storage systems, etc.), migration from a physical to virtualized environment, the migration from an on premise to a cloud hosted environment, any application configuration changes, the establishment of new network segments, and the establishment of third party interconnections.

**SA-05: SECURITY ASSESSMENT**

The NJOHSP Division of Cybersecurity shall be responsible for conducting security assessments for any new major applications, general support systems, and external connections, as well as any major applications, general support systems, and external connections in development, or undergoing substantive changes. The assessment shall be conducted in three (3) phases:

(a) **Initiation and Planning**: Upon submission of a Privacy Impact Assessment the NJOHSP Division of Cybersecurity will review and assess the risks and provide guidance regarding security requirements necessary to manage the risks to acceptable levels.

(b) **Certification**: In conjunction with the Information System Owner and the Agency CISO the NJOHSP Division of Cybersecurity shall review and assess the System Security Plan to ensure information security risks are addressed and the system is being constructed in compliance with the policies and standards contained in this Manual, agency-specific policies and standards, applicable State and Federal legal requirements, and regulatory and contractual obligations. Security deficiencies identified shall require revision of the SSP until they are certified as sufficient by the NJOHSP Division of Cybersecurity.

(c) **Accreditation**: In conjunction with the Information System Owner and the Agency CISO, the NJOHSP Division of Cybersecurity shall conduct an assessment of the system’s security controls to validate the controls certified in the SSP have been implemented. The audit may include interviews, vulnerability scans, visual inspections, and penetration tests. The audit shall occur concurrent with the NJOIT System Architecture Review (SAR) process Implementation Review.

Guidelines: Agencies should implement risk management processes throughout the life cycle of an information system. This includes identifying, assessing, and addressing security risks at the inception of the project to build a system, through to decommissioning of a system. By including risk management practices at the inception of a system project, agencies can implement security by design, thereby ensuring security certification and accreditation, and implementation into an operational status, more efficiently.
SA-06: AUTHORITY TO OPERATE

Based on the results of the security assessment the State Chief Information Security Officer, or his/her designee, shall provide the Information System Owner with one of the following three designations for the system under review:

Authority to Operate (ATO) – The ATO is a formal designation and determination by the State Chief Information Security, or his/her designee, that the security controls for the system under review have been certified and accredited as being compliant with the policies and standards contained in this Manual, the agency-specific policies and standards, and applicable State and Federal laws, and regulatory and contractual obligations. An ATO designates that the system may be implemented into the production environment for its intended purpose, pending approval from the NJOIT CTO, or his/her designee. An ATO for a given system shall be effective for a period of three (3) years, pending the implementation of continuous monitoring processes that address new threats and manage risks during that period.

Interim Authority to Operate (IATO) - The IATO is a temporary designation and determination by the State Chief Information Security, or his/her designee, that some of the security controls for the system under review have not been certified and accredited as being compliant with the policies and standards requirements contained in this Manual, the agency-specific policies and standards, and/or applicable State and Federal laws, and/or regulatory and contractual obligations. An IATO designates that the system may be implemented into the production environment for its intended purpose so long as the system is brought into compliance within a designated time period, and pending approval from the NJOIT CTO, or his/her designee. Systems that receive an IATO are required to be re-assessed upon remediation of the identified security deficiencies.

Denied Authority to Operate (DATO) – the DATO is a designation and determination by the State Chief Information Security, or his/her designee, that the security controls for the system under review have not been certified and have not been accredited as being compliant with the policy and standards contained in this Manual, the agency-specific policies and standards, and/or applicable State and Federal laws, and/or regulatory and contractual obligations. The system’s implementation into the production environment would likely result in a loss of confidentiality, integrity, availability, privacy, or safety and have severe or catastrophic adverse effects on the Agency’s or State’s operations, organizational assets, or individuals. A DATO designates that the system may not be implemented into the production environment. Systems that receive a DATO are required to be re-assessed upon remediation of the identified security deficiencies.

SA-07: CONTINUOUS MONITORING REQUIREMENT

In order to establish and maintain situational awareness and the ability to address new threats to the security of a system that has received an ATO or and IATO, agencies are responsible for implementing continuous monitoring processes. Continuous monitoring processes include, but are not limited to: the ongoing monitoring of system security logs and audit events, the conduct of periodic risk assessments and vulnerability scans, and the application of security patches based on new vulnerabilities or threats that are identified. The failure to implement continuous monitoring processes may result in the loss of a system’s ATO or IATO designation.
Guidelines: Additional information regarding continuous monitoring processes can be found in the Continuous Monitoring Policy, the Risk Management Policy, and the Vulnerability and Patch Management Policy.

REFERENCES
The requirements established in the Security Assessment and Authorization Policy have been derived from the following:

- NIST SP 800-53 Security Assessment and Authorization (CA); and
- NIST CSF Identify/Risk Assessment (ID.RA), Identify/Risk Management (ID.RM), Detect/Security Continuous Monitoring (DE.CM).
EXCEPTION MANAGEMENT (EX)

PURPOSE
The purpose of the Exception Management Policy is to establish processes for the submission, review, documentation, and application of exceptions to compliance with the information security policies and standards when a valid business reason exists.

KEY TERMS
Exception: an adjudicated exemption to compliance with an information security policy, standard, procedure, or practice.

EX-01: POLICY
Agency personnel are required to comply with the information security policies and standards documented in this Manual, which are designed to establish the controls necessary to manage risk at acceptable levels. A control deficiency in one agency process or information asset can jeopardize the security of other processes or assets as the deficiency may act as a conduit to a loss of confidentiality, integrity, availability, and/or privacy in State information and information systems. In cases where compliance with the information security policies and standards cannot be achieved for a valid reason, an exception request must be submitted and approved prior to an exemption from compliance being granted.

This policy is supported by the following standards and guidelines.

EX-02: EXCEPTION REQUEST SUBMISSIONS
Agencies shall be responsible for documenting, approving, and assuming any risk of loss of confidentiality, integrity or availability of an Agency's information assets, due to the inability to comply with a policy, standard or procedure. The Agency must fully describe the risk, and how the Agency is ensuring that all necessary compensating controls have been implemented, and how the exception will be monitored.

All requests for compliance exceptions must be based on a valid restriction that prevents full compliance with the policy, standard or procedure. Exception requests must be approved by the Agency CIO or CISO and forwarded to the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and the New Jersey Office of Information Technology (NJOIT) for acceptance and cataloging.

Guidelines: Exceptions are to be considered only when a valid business reason exists. Valid business reasons may include, but are not limited to, the following situations:

- Temporary exception, where immediate compliance would disrupt essential business operations;
- Another acceptable solution with equivalent protection is available;
• A superior solution is available;
• A legacy system has technical limitations for which compliance is not possible (risk must still be managed);
• Long-term exception, where compliance would adversely impact essential Agency or State business; and/or
• Compliance would cause an adverse financial impact that would not be offset by the reduced risk produced by compliance (i.e., the cost to comply offsets the risk of non-compliance).

Exceptions will not be granted for convenience reasons.

**EX-03: EXCEPTION REQUEST REQUIREMENTS**

The requestor of an exception to a policy, standard, or procedure shall document, at a minimum, the following information in the Information Security Exception Request Form:

• A specific description of the exception and the policy, standard or procedure for which the exception is requested;
• Why the policy, standard or procedure cannot be implemented, and the proposed alternative measures or compensating controls to be implemented;
• The proposed exception duration, with a specific date for remediation, which can be no longer than one year from the date of the exception request;
• The Criticality and Sensitivity of Data or Hardware involved in the exception; and
• The requestor will forward the request to their Agency CIO/CISO for approval and signature.

Guidelines: Agencies should maintain documentation describing the functional limitations and the mechanism employed to mitigate the risk. The exception shall be considered temporary and NJOHSP shall track and review exceptions for as long as they exist, to determine if the exception is still required, if the Agency has means to correct the exception, or if alternative mechanisms can be put in place to remediate the exception.

**EX-04: REQUEST DETERMINATIONS**

Exception requests will be considered on a case-by-case basis.

The Agency Chief Information Security Officer (CISO) and his/her designated representatives will review the request from the Agency requestor and, if they approve, will sign and forward to the State Chief Information Security Officer at the NJOHSP Division of Cybersecurity for review, via RiskReview@cyber.nj.gov.
The State Chief Information Security Officer, or his/her designee, upon receiving the request for exception, shall:

(a) Review and determine:
   (1) The validity of the request as it relates to the overall Statewide Information Security Manual goals and objectives, and any risk mitigation considerations or compliance mandates that impact the request;
   (2) Whether the exception violates any dominant policy, statutory, regulatory or known contractual compliance obligation (e.g., Federal or State);
   (3) Whether granting the exception would likely result in a loss of confidentiality, integrity, availability, privacy, or safety and have serious adverse effects on the Agency’s or State’s operations, organizational assets, or individuals;
   (4) Whether the proposed alternative measures provide compensating controls necessary to appropriately manage risk;
   (5) Whether other alternative approaches for handling the requested exception may be available for consideration; and
   (6) Whether the proposed plan and timeframe for corrective actions are reasonable given the risk.

(b) Solicit input from key management and business units that may be affected by the exception;

(c) Forward the exception to the NJOIT Information Security Officer, or his/her designate, for review with related systems managed by NJOIT, and for a coordinated decision. The NJOIT ISO shall:
   (1) Determine the potential impact the exception request may have on any other NJOIT managed information assets;
   (2) Indicate their approval of the request for exception if no expected extra-Agency security risks to NJOIT managed information assets exist;
   (3) Indicate disapproval if there would be expected extra-Agency security risks to NJOIT managed information assets;
   (4) Indicate conditional approval of the request for exception and specify any additional actions required by the requesting Agency in order to comply; and
   (5) Return the request with their decision to the State CISO for final review and handling;

(d) Accept the review from the NJOIT ISO and coordinate with the Agency CIO/CISO and the requestor to ensure that the appropriate alternative control methods agreed upon in granting the exception have been implemented, and that the request is still valid. If approved, the exception is signed and returned to the Agency CISO. If disapproved, the exception is returned to the Agency CISO and the requestor;
(e) After final review, approve or disapprove of the request for exception and notify the requestor, and also inform the State Chief Technology Officer and NJOIT CISO. The NJOHSP Division of Cybersecurity shall maintain copies of, and track, all exceptions; and

(f) Review approved exceptions with the Agency requestor on an on-going basis (no less than annually), to determine if the exception is still required and valid.

Should the State Chief Information Security Officer disapprove the request for exception, the requestor will have 90 days to comply with the policy, standard or procedure.

Guidelines: Agencies should make all efforts to manage risks at acceptable levels commensurate with the sensitivity and criticality of the information asset. Exceptions that may jeopardize the security of multiple agencies’ or statewide information assets may require additional review, up to and including, the Information Security Governance Committee.

**EX-05: PERIODIC REVIEW**
On an on-going basis (no less than annually), the State Chief Information Security Officer, or his/her designee, shall review all outstanding exceptions with the Agency CIO/CISO or requestor to determine if the exception is still required and valid.

Any policy exception request more than one year old will require a new request to be submitted for an updated review and determination.

**REFERENCES**
The requirements established in the Exception Management Policy have been derived from the following:

- NIST SP 800-53 Security Assessment and Authorization (CA); and
- NIST CSF Protect/Information Protection Policies and Procedures (ID.PR).
PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

PURPOSE
The purpose of the Physical and Environmental Security Policy is to minimize risk to State information systems and information by addressing applicable physical security and environmental concerns.

KEY TERMS
Authorization - Access privileges granted to a user, program, or process or the act of granting those privileges.

PE-01: POLICY
Agencies shall establish documented physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. Agencies shall provide appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions.

This policy is supported by the following standards and guidelines.

PE-02: PHYSICAL ACCESS SECURITY ZONES
Agencies shall establish their premises into areas (zones) with differing levels of security as required to allow for access by authorized personnel. The fundamental principle behind this zoning is to have multiple layers of physical security protecting the most critical assets and services.

There are four main categories of zones:

(a) Public Zone - Areas of an agency facility accessible by the general public either by vehicles or pedestrians without prior control, such as grounds, parking lots and other areas of the facility. Property limits should be clearly identified. Information labeled Confidential, as defined in this Manual, must not be left unattended in Public Zones.

(b) Reception Zone - An area at the entrance point of an agency building where the initial contact with representatives of the agency occurs (e.g., receptionist, Physical Security personnel). Although certain basic business activities can be conducted in Reception Zones, their main purpose is to provide an adequate environment for identification and access control.

(c) Operations Zone - An operations zone is a general access area where agency daily business activities or support services are regularly conducted. The basic security objective is to ensure that access and movement within this zone is limited to authorized personnel.
Access to operations zones requires appropriate credentials (Visible ID badge, proximity card, combination, or keys) and is limited to:

1. Authorized employees (all employees of a particular location);
2. Authorized and adequately supervised contractors; and
3. Properly escorted visitors.

Access to an operations zone from a public zone should be properly labelled (e.g. “Restricted area. Employees only!”)

(d) **Restricted Access Zone** - A restricted access zone is defined as an operational zone that requires specific authorization granted by the owner of each restricted zone. Restricted access zones could be areas such as data centers, server or computer rooms, cable cabinets, and communication equipment rooms. Not all operations zone personnel have access to restricted access zones. As a general rule, restricted access zones should not be directly accessible from public zones.

Restricted access zones include a combination of enhanced security measures to ensure that:

1. Access privileges are limited to specifically authorized employees, contractors, and escorted visitors based on their need;
2. Unauthorized access is detected, and prompt and appropriate intervention action is taken; and
3. The areas are monitored as a detective security control.

Controlling physical access to restricted access zones is required and access must be based on an individual’s job function.

Access to restricted access zones must be revoked immediately upon termination, and all physical access mechanisms, keys, access badges, or tokens, must be returned or disabled.

Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls.

Guidelines: The security zone categories represent descriptions of their purpose.

**PE-03: PHYSICAL ACCESS AUTHORIZATION**

Access to the non-public areas of agency facilities shall be granted to only authorized personnel.

(a) Agency employees shall be provided authorized access to Operations and Restricted security areas within agency facilities based on their roles and responsibilities;

(b) Agencies are required to maintain records documenting the authorization and provisioning of physical access to agency facilities;
(c) Agencies shall establish procedures to ensure employees and other authorized individuals understand the security procedures and safeguards related to the zones to which they have access; and

(d) With the exception of areas that are designated as publicly accessible, agencies shall maintain a list of personnel with authorized access to a facility or a secure area within the facility where agency information assets reside.

Guidelines: All personnel seeking access to secured areas and facilities should have a badge or key for entry, which they may obtain through their agency Human Resources Department or the Facilities Manager. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Agencies are to determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or system users.

Agency procedures should include prohibitions against “tailgating”, the process of allowing unauthorized entry by those who follow through open doors or gates, and propping open doors or disabling automated closing mechanisms.

**PE-04: VISITOR CONTROL**
Physical access to the operations and restricted areas of agency facilities by visitors shall be restricted and controlled in order to prevent unauthorized access to agency information assets. Other than areas designated as publicly accessible, all visitors shall be approved and authenticated before access to agency operations or restricted zones.

Individuals escorting visitors are responsible for ensuring that the visitors:

(a) Wear their visitor security badge at all times; and

(b) Are escorted until they are signed out.

**PE-05: LOST OR STOLEN ID BADGES**
 Agencies shall establish procedures for badge holders to report any loss or theft of their ID badge. Lost or stolen badges are to be immediately deactivated to prevent unauthorized access to agency facilities.

**PE-06: PHYSICAL ACCESS CONTROLS**
 Agencies shall implement physical access controls at all physical access points, including designated entry/exit points, to agency facilities and secured areas within the facilities where information assets reside, excluding those areas within the facility officially designated as publicly accessible. These physical access controls include:

(a) Security perimeters (i.e. barriers such as walls, card-controlled entry gates, or manned reception desks);
(b) Validation of individual access authorization before access is granted (e.g. identity and authorization controls, security badges, biometrics, etc.);

(c) Control of access to agency facilities and areas shall be restricted in accordance with an assessment of risk;

(d) Secure keys, combinations, and other physical access devices shall be implemented to restrict access to only authorized personnel;

(e) Inventory and review of physical access devices on an annual basis; and

(f) Procedures that require the changing of combinations and keys when keys are lost, combinations are compromised, or certain individuals are transferred or terminated.

Guidelines: Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within agency facilities include, for example, cameras, monitoring by guards, isolating selected systems/components in secured areas.

**PE-07: SECURITY MONITORING AND AUDITING OF PHYSICAL ACCESS**

As applicable to mitigate risks of unauthorized physical access to information assets and to ensure compliance with applicable policy, contractual, regulatory, and statutory requirements, agencies shall implement security monitoring technologies and systems.

Agency personnel assigned to publicly accessible facilities shall periodically review and audit the physical security of agency information assets located in publicly accessible areas to detect any signs of unauthorized access, tampering, destruction, or theft.

Guidelines: Examples of security monitoring technologies and systems include, but are not limited to, closed circuit video systems, alarms, and intrusion detection systems, card-controlled entry systems, etc. As permissible by law, agency security monitoring systems and authorized agency personnel may monitor, record, audit, review, and log any physical access to its facilities and areas within said facilities.

**PE-08: RETENTION OF SECURITY LOGS AND VIDEO**

Agencies are required to develop processes to ensure all audit logs of badge access and video from closed circuit video cameras that document access to agency facilities are retained in accordance with applicable statutory, regulatory, contractual, and State policy requirements.

To allow for the auditing of physical access and/or the investigation of security incidents, the following minimum retention requirements shall be adhered to:

(a) Audit logs of badge access and video from closed circuit video cameras that document access to agency facilities are to be retained for no less than ninety (90) days;

(b) Audit logs of badge access and video from closed circuit video cameras that document access to restricted access zones such as data centers, server rooms, and other such areas are to be retained for no less than one (1) year; and
(c) Visitor sign-in/sign-out logs shall be retained for a minimum of one (1) year.

Guidelines: The retention requirements listed above represent the minimum necessary to allow for effective security, auditing, and investigation in the event of an incident. State data retention requirements, as well as other policy, statutory, regulatory, or contractual requirements may require longer retention periods. Agencies should review all statutory or regulatory retention requirements applicable to their facilities and the information that is processed or stored within them.

**PE-09: LOCATION OF INFORMATION ASSETS**

Agency information assets and their respective components must be positioned within a facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

Guidelines: Individuals who access sensitive information should position their monitors so that sensitive information is not visible to unauthorized individuals. The use of screen protectors should be considered in open work areas.

**PE-10: CLEAN DESK/CLEAN SCREEN REQUIREMENTS**

Sensitive information, whether in paper or electronic form, must be protected from unauthorized access and disclosure.

Guidelines: When sensitive information is to be left in an unattended location, it should be secured in file cabinets or other appropriate containers. During non-working hours, desks should be cleared to prevent unauthorized access and disclosure of sensitive information. To prevent unauthorized access to, or duplication and transmission of sensitive information, documents containing such information should not be left unattended on printers, copiers, or fax machines.

**PE-11: POWER EQUIPMENT AND POWER CABLELING**

All agency facilities must protect the power equipment and power cabling for information assets from damage and destruction.

**PE-12: EMERGENCY SHUTOFF**

All agency facilities must be able to shut off power to information assets or individual asset components in emergency situations. In addition, emergency shutoff switches or devices must be placed in clear and accessible areas to facilitate safe and easy access for personnel.

**PE-13: EMERGENCY POWER**

Short-term, uninterruptible power supplies to facilitate an orderly shutdown of information assets in the event of a primary power source loss, should be implemented based on the criticality of the information asset and business operations.
PE-14: EMERGENCY LIGHTING
All agency facilities must employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption, and that indicates emergency exits and evacuation routes within the facility.

PE-15: FIRE PROTECTION
All agency facilities must employ and maintain appropriate fire suppression and detection devices/systems.

PE-16: TEMPERATURE AND HUMIDITY CONTROLS
All agency facilities must maintain temperature and humidity levels within the facility where the information asset resides, at operational levels. In addition, temperature and humidity monitoring must be on-going.

PE-17: WATER DAMAGE PROTECTION
All agency data processing facilities and data centers must protect information assets from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

PE-18: DELIVERY AND REMOVAL OF INFORMATION ASSETS
Agencies shall develop procedures for the delivery and removal of information assets to and from agency facilities.

(a) Agency equipment, information, and/or software shall not be taken off-site without documented prior authorization; and

(b) All Agency facilities must authorize, monitor, and control shipments and equipment removals from the facility and maintain records of those items.

PE-19: SECURING PORTABLE INFORMATION ASSETS
Individuals who are provided with portable information assets, including but not limited to: laptop computers, tablets, smart phones, removable media, etc., shall be responsible for the physical security and condition of these information assets. When an information asset is allocated to an individual, the individual assumes temporary custodianship of the asset.

Agency information assets issued to employees and contractors shall remain the property of the agency.

At a minimum, users of agency portable information assets shall take the following physical security preventative measures:

(a) Portable information assets shall not be left in view in an unattended vehicle;

(b) Portable information assets shall not be left in an unattended vehicle (in or out of view) overnight;
(c) Portable information assets displaying sensitive information should be positioned, whenever possible, so that the screen cannot be viewed by others;

(d) When leaving a portable information asset unattended in a hotel room, users shall physically secure it with a cable lock and/or lock it in a safe or cabinet;

(e) In vulnerable situations, i.e., public areas such as airport lounges and conference centers, the portable information assets shall never be left unattended;

(f) Portable information assets shall, whenever permitted, be carried as hand luggage when traveling; and

(g) All portable information assets (laptops, tablets, smart phones, removable media, etc.) that contain sensitive information shall be encrypted.

Guidelines: Laptops or other mobile devices should never be left in the passenger compartment of an unattended vehicle.

**PE-20: DISPOSAL/TRANSFER OF INFORMATION ASSETS**
Information assets shall be disposed of, or reassigned, in a manner that does not compromise the security of the asset, and in accordance with the Media Protection Policy as documented herein.

**REFERENCES**
The requirements established in the Configuration Management policy have been derived from following:

- NIST SP 800-53 Physical and Environmental Policies and Procedures (PE); and
- NIST CSF Protect/Data Security (PR.DS), Detect/Security Continuous Monitoring (DE.CM).
CONTINGENCY PLANNING (CT)

PURPOSE
The purpose of the Contingency Planning Policy is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability.

KEY TERMS
Recovery Point Objective (RPO) - The point in time to which data must be recovered after an outage.

Recovery Procedures - Actions necessary to restore data files of an information system and computational capability after a system failure.

Recovery Time Objective (RTO) - The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes.

CT-01: POLICY
Agencies are required to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the State of New Jersey.

This policy is supported by the following standards and guidelines.

CT-02: CONTINGENCY PLAN
Agency CIOs shall develop contingency plans that:

(a) Identify and document essential mission and business functions and the associated contingency requirements;

(b) Provide recovery objectives, restoration priorities, and metrics;

(c) Address contingency roles, responsibilities, and emergency contact information;

(d) Address maintaining essential missions and business functions in the event of information system disruption, compromise, or failure;

(e) Address eventual, full information system restoration without deterioration of the related security safeguards;

(f) Address resumption of essential missions and business functions within a time frame specified by the Agency CIO and based on mission needs, applicable laws and regulations, and applicable contracts and agreements with other State agencies or external organizations; and
(g) Identify and document critical information system assets supporting organizational missions and business functions.

Guidelines: In accordance with the Organizational Security Policy Agency CIOs in coordination with the NJoit and the State CTO are responsible for disaster recovery planning and operations. The development of business continuity planning and plan development should be established, documented, and adopted to ensure all business continuity plans address priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans should include the following:

- Defined purpose and scope, aligned with relevant dependencies;
- Accessible to, and understood by, those who will use them;
- Owned by agency CIO or State CTO who is responsible for their review, update, and approval;
- Defined lines of communication, roles, and responsibilities;
- Detailed recovery procedures, manual workaround, and reference information; and
- Method for plan invocation.

**CT-03: MANAGEMENT OF CONTINGENCY PLANS**

On an ongoing basis, agencies shall manage their contingency plans by carrying out the following activities:

(a) Distributing the contingency plans to key contingency personnel, including those contingency personnel within other State agencies and external entities, including business partners, vendors, and service providers that provide support for, or are responsible for implementing the plans;

(b) Coordinating contingency planning activities with information security incident handling activities;

(c) Reviewing the contingency plans annually;

(d) Revising the contingency plans to address changes to the State or the agency, agency information systems, operational environment or problems encountered during plan implementation, execution or testing;

(e) Communicating contingency plan changes to key contingency personnel; and

(f) Protecting the contingency plans from unauthorized disclosure and modification.

**CT-04: CONTINGENCY PLAN TESTING AND EXERCISES**

Business continuity plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Agencies are required to:

(a) Establish and implement periodic testing procedures;
(b) Test their contingency plan to determine the plan’s effectiveness and the agency’s readiness to execute the plan;
(c) Document the contingency plan test results; and
(d) Involve and coordinate contingency plan tests and exercises with impacted customers and all key stakeholders, as applicable.

Guidelines: Agency CIOs should coordinate contingency plan testing for each agency information system with all key stakeholders including customers, and other State agencies, business partners, vendors, and service providers that provide support for, or are responsible for implementing the plan.

CT-05: CONTINGENCY TRAINING
Agencies shall develop and provide contingency training to agency personnel consistent with their assigned roles and responsibilities.

Guidelines: Contingency training provided by agencies is linked to the assigned roles and responsibilities of agency personnel to ensure the appropriate content and level of detail is included in such training. For example, users may only need to know when and where to report for duty during contingency operations if normal duties are affected; system administrators may require additional training on how to set up systems at alternate processing and storage sites; and managers and executive management may receive more specific training on how to conduct mission essential functions in designated off-site locations and how to establish communications with other entities for purposes of coordination of contingency-related activities.

CT-06: ALTERNATE SITE
Agencies shall establish alternate sites for storage, processing, and communications functions including necessary agreements to permit the recovery from, and resumption of, agency information system operations for essential mission and business functions consistent with the agency’s recovery time and recovery point objectives for when the primary site’s storage, processing, or communications functions are unavailable.

Agencies shall:
(a) Ensure that equipment and supplies necessary to transfer and resume operations are available at the alternate site, or contracts are in place to support delivery to the site in time to support the agency’s defined period for transfer/resumption;
(b) Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site;
(c) Ensure that the alternative storage site is geographically separated from the primary storage site to reduce susceptibility to the same hazards; and
(d) Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
Guidelines: Agencies should consider geographic diversity when considering alternate sites to ensure hazards that may impact the primary site do not impact the alternate site. And while geographic diversity may allow for the alternate site not to be affected by power or communications issues impacting the primary site, the distance to the alternate site for key personnel supporting recovery activities should also be considered.

CT-07: INFORMATION SYSTEM BACKUP
Agencies shall conduct backups, consistent with the agency’s recovery time and recovery point objectives, of user-level and system-level information contained in agency information systems, and agency information system documentation, including security-related documentation.

Agencies shall:
(a) Ensure the protection of the backup information consistent with its security categorization;
(b) Test backup information at least annually to verify media reliability and information integrity; and
(c) Document the results of the backup tests.

CT-08: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
Agencies shall provide for the recovery and reconstitution of the agency information systems to a known state after a disruption, compromise, or failure.

Guidelines: Recovery is executing system contingency plan activities to restore agency mission and business functions. Reconstitution takes place following recovery and includes activities for returning agency systems to fully operational states.

CT-09: CONTINGENCY PLAN ROOT CAUSE ANALYSIS
Agencies shall perform a root cause analysis following events that trigger implementation of continuity plans. The lessons learned are to be incorporated into updates to the contingency plans.

CT-10: CONTINGENCY PLAN UPDATE
Agencies shall implement procedures to ensure that:
(a) Agency contingency plans are reviewed at least once a year;
(b) Contingency plan tests and exercise results are reviewed;
(c) Lessons learned from the implementation of the plan are included in the updates.
REFERENCES

The requirements established in the Contingency Planning policy have been derived from the following:

- NIST SP 800-53 Contingency Planning (CP), Program Management (PM); and
INCIDENT RESPONSE (IR)

PURPOSE
The purpose of the Incident Response Policy is to establish a consistent and organized approach for preparing for, identifying, reporting, and managing information security incidents that may compromise the confidentiality, integrity, availability, and privacy of the State’s information and information systems.

KEY TERMS
Incident - An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation, or imminent threat of violation of security policies, security procedures, or acceptable use policies.

IR-01: POLICY
Agencies shall maintain an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

This policy is supported by the following standards and guidelines.

IR-02: REPORTING INFORMATION SECURITY INCIDENTS
All agency personnel who are provided authorized access to agency information assets are responsible for promptly reporting suspected or actual security incidents.

(a) Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
- Agency IT Service Desk;
- Agency CISO;
- Agency HR Representative;
- NJOIT Enterprise Service Desk – 1.800.622.4357; and/or

(b) Upon notification from a user of a suspected information security incident the receiving entity will document the information provided and notify the Agency CISO or a designee, of the report; and

(c) Agencies shall report all incidents to the New Jersey Cybersecurity Communications and Integration Cell for de-confliction, trending, and assistance in responding to an incident.
Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to, and including termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

**IR-03: INCIDENT RESPONSE PLANNING**

The State Chief Information Security Officer (CISO) shall be responsible for the development, maintenance and promulgation of a Statewide Information Security Incident Response Plan. Agencies are responsible for incorporating the strategies included in the statewide plan into their respective agency incident response plans.

(a) The Information Security Incident Response Plans shall encompass strategies for incident response preparation; detection and analysis; containment, eradication, and recovery; and post-incident analysis, in accordance with the NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*;

(b) The plans shall define the roles and responsibilities of incident response team participants, the characterization of incidents, relationships to other policies and procedures, and reporting requirements;

(c) The State CISO shall be responsible for the development of a Statewide incident response training curriculum, to include table-top or simulation exercises to aid agencies in effectively responding to incidents. Agency CISOs are responsible for training activities within their respective agencies; and

(d) Agency Heads shall be responsible for the implementation of the Information Security Incident Response Plan within their respective agencies, including the designation of an agency Information Security Incident Response Team (ISIRT) and an individual with responsibility to act as the agency’s ISIRT Coordinator for the agency.

Guidelines: Training should incorporate simulated events and tests or exercises of the agency’s and the State’s incident response capabilities. Incident response training should be linked to the assigned roles and responsibilities of agency personnel. Role-based training for the agency’s ISIRT team and incident identification and reporting for all agency personnel should be training priorities.

**IR-04: INCIDENT RESPONSE TEAM**

Agency CISOs shall establish an agency Information Security Incident Response Team (ISIRT) that is charged with promptly and correctly handling information security incidents that may impact the agency, including its systems, networks, services, data, customers, and employees.

(a) The ISIRT should be comprised of capable members from the agency IT team, agency information security team, the agency legal representative, the agency public information office, the agency human resources department, and auxiliary functions or resources, as necessary;
(b) Agencies shall assign an ISIRT Coordinator who is responsible for coordinating the response of the agency ISIRT and for communicating or escalating the incident as appropriate;

(c) The ISIRT is responsible for carrying out the agency’s response to information security incidents;

(d) The ISIRT is authorized to take the appropriate steps deemed necessary to contain, mitigate, and resolve an information security incident in an effective and efficient manner;

(e) The ISIRT is authorized to take necessary action to protect agency information assets or preserve evidence;

(f) The incident’s classification, severity, and other factors will dictate which ISIRT members are required to respond to an incident. From the time an incident is reported the ISIRT, members who have received the report are responsible for:

   (1) Validating the initial report and declaring an incident as appropriate;
   (2) Determining the type, severity, and priority of the incident; and
   (3) Notifying the ISIRT Coordinator or an authorized designee of the incident;

(g) The ISIRT Coordinator will determine which ISIRT members play an active role in the response and:

   (1) Coordinate the agency’s response efforts;
   (2) Engage auxiliary agencies and resources as necessary;
   (3) Escalate incidents to executive management as appropriate;
   (4) Monitor progress of the response;
   (5) Ensure evidence gathering, chain of custody, and preservation is appropriate;
   (6) Manage all communications with outside organizations (i.e., law enforcement, media, and regulatory bodies);
   (7) Manage all communications with external Agencies such as NJOIT and NJCCIC; and
   (8) Prepare a written summary of the incident and corrective action taken.

Guidelines: The agency ISIRT Coordinator is typically the agency CIO or CISO. It should be an individual with the ability and authority to make decisions regarding the overall management of an information security incident. The ISIRT Coordinator must understand all facets of incident handling. The ISIRT is to be comprised of individuals with the skills and abilities to effectively handle and incident.

As necessary to effectively respond to an incident, the agency ISIRT will be supported by the New Jersey Cybersecurity and Communications Integration Cell and the New Jersey Office of
Information Technology. For agencies that do not have the resources to handle information security incidents, the NJCCIC can provide incident response assistance. Depending on the nature and severity of the incident the State CISO or his/her designee may assume the role of the ISIRT Coordinator.

In accordance with Executive Order 178 (Christie 2016), the NJCCIC may draw upon the assistance of any department, office, division, or agency of this State to supply it with expertise and assistance, including information and personnel, when responding to a cybersecurity incident.

**IR-05: INCIDENT CATEGORIZATION**

To ensure a consistent approach to the reporting, response, handling, and tracking of incidents, agencies will use the following categorizations to describe the type of incident.
<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat 0</td>
<td>Security Testing</td>
<td>This category is used during agency approved vulnerability and penetration testing activities and other security exercises intended to test the network defenses or responses.</td>
</tr>
<tr>
<td>Cat 1</td>
<td>Unauthorized Access</td>
<td>An individual gains logical or physical access, without authorization to an agency network, system, application, private or restricted data, or other information asset.</td>
</tr>
<tr>
<td>Cat 2</td>
<td>Denial of Service (DoS)</td>
<td>An attack that successfully prevents or impairs the normal authorized functionality of agency networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.</td>
</tr>
<tr>
<td>Cat 3</td>
<td>Malicious Code</td>
<td>Successful installation of malicious software (e.g., virus, worm, Trojan horse, ransomware, or other code-based malicious entity) that infects an agency operating system or application.</td>
</tr>
<tr>
<td>Cat 4</td>
<td>Improper Usage</td>
<td>A user violates the Rules of Behavior - Acceptable Use of State Information Assets Policy or other agency or State policies.</td>
</tr>
<tr>
<td>Cat 5</td>
<td>Scans, Probes, Attempted Access</td>
<td>Any activity that seeks to access or identify an agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.</td>
</tr>
<tr>
<td>Cat 6</td>
<td>Investigation</td>
<td>Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.</td>
</tr>
<tr>
<td>Cat 7</td>
<td>Data Breach</td>
<td>A Data Breach is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The compromise of the confidentiality of personally identifiable information;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The loss of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of personally identifiable information;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access to personally identifiable information that is for an unauthorized purpose; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access to personally identifiable information that is in excess of authorization.</td>
</tr>
</tbody>
</table>

Incidents that may include activity spanning across multiple categories will be classified according the category associated with the highest severity level.
IR-06: INCIDENT SEVERITY AND PRIORITIZATION

Agencies shall classify the severity of the incidents using one of the following three (3) levels:

(a) High;
(b) Medium; or
(c) Low.

Guidelines: The severity of an information security incident determines the priority and resources necessary to handle the incident. It also determines the timing and extent of the response, the documentation and communications. Severity is a subjective measure of the incident’s impact on, or threat to, the confidentiality, integrity, availability, and privacy of agency information and information assets. An incident’s severity level may be revised throughout the various incident response phases as dictated by information that is developed.

Agencies must consider the following factors when determining the severity of an incident:

- Threat to human safety;
- Scope of impact – number and criticality of systems, services, agencies and people affected;
- Financial impact to the agency or State – loss of revenue, financial penalties, etc.;
- Sensitivity of the information – personally identifiable information (PII) or other sensitive information;
- Probability of propagation - likelihood that the malware or negative impact will spread, or propagate, to other systems or agencies;
- Reputational impact to the State or an individual agency; and
- Legal obligations and risks - notification requirements, regulatory issues, potential lawsuits, etc.

Other factors beyond those listed above may affect the severity rating of an incident.

IR-07: INCIDENT TRACKING, DOCUMENTATION AND REPORTS

Agencies shall establish procedures to ensure all incident response activities are documented to include artifacts and evidence obtained using methods consistent with chain of custody and confidentiality requirements.

(a) Documents and artifacts associated with incidents shall be protected commensurate with their sensitivity and are to be protected from tampering;

(b) Agencies shall establish processes for recording and maintaining incident reports;

(c) The NJCCIC shall be responsible for developing and maintaining a centralized incident tracking system to aid in enhancing the response to incidents and their prevention; and
(d) All agencies shall report all incidents to the NJCCIC for entry into the incident tracking system.

Guidelines: Individual security incidents may require completion of an incident report that provides a summary of the incident, its resolution, and any recommendations to help mitigate the risk of a reoccurrence.

REFERENCES
The requirements established in the Incident Response Policy have been derived from the following:

- NIST SP 800-53 Incident Response (IR);
- NIST CSF Protect/Information Protection Processes and Procedures (PR.IP), Detect/Anomalies and Events (DE.AE), Respond/Response Planning (RS.RP), Respond/Analysis (RS.AN), Respond/Mitigate (RS.MI), Respond/Communications (RS.CO); and
- NIST Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide.
APPENDIX A – SECURITY CATEGORIZATION CONSIDERATIONS

The considerations listed below must be evaluated by agencies when assigning security categorizations to their information assets and determining the impact should a loss of confidentiality, integrity, availability, or privacy be realized.

(a) **Legal, Regulatory, Contractual, and Policy Compliance** - Various federal and state laws, regulations, contracts and policies mandate the protection of personal information from unauthorized access, use, or disclosure. Questions regarding laws and regulations that apply to specific agencies and the information they collect, store, process, or output should be directed to the agency’s legal counsel (Office of the Attorney General).

(b) **Personal Information** – New Jersey Revised Statutes §56:8-161 (2013) defines Personal Information as an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver’s license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

(c) **Personally Identifiable Information (PII)** - NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an agency, including

1. any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and

2. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include but are not limited to the following:

- Name, such as full name, maiden name, mother’s maiden name, or alias Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
• Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);

• Information identifying personally owned property, such as vehicle registration number or title number and related information; and

• Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

(d) **Sensitive Personally Identifiable Information (SPII)** - Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

(e) **Criminal Justice Information** - is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

• Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

• Identity History Data - textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

• Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

• Property Data - information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

• Case/Incident History - information about the history of criminal incidents.

(f) **Federal Tax Information (FTI)** - FTI consists of federal tax returns and return information (and information derived from it) that is in the agency’s possession or control which is covered by the confidentiality protections of the *Internal Revenue Code* (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.
FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

(g) **Electronic Protected Health Information (ePHI)** – Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that can be linked to an individual. PHI refers to all “individually identifiable information” held or transmitted by the State Entities or its business associates in any form or media, whether paper, electronic or oral. “Individually identifiable health information” is information, including demographic data, that relates to:

- The individual’s past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- The individual’s identity or for which there is a reasonable basis to believe it can be used to identify the individual.

(h) **Social Security Administration Provided Information** – is information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

(i) **Payment Card Industry (PCI) Data Security Standard (DSS) Information** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

(j) **Potential Harm to Individuals** - Agencies must consider any potential harm or adverse impact that the compromise of information may have on the parties to whom the information pertains.

(k) **Agency Mission and Business Objectives** - Agencies must consider their mission and business objectives when assigning information classifications. Certain agencies may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the agency to ensure that those objectives are met, adequate controls need to be in place and in effect to address confidentiality, integrity, availability, and privacy.

(l) **Information System Dependencies/Connections and Aggregation/Commingling of Information** - Agencies must consider the risks associated with information system dependencies and connections to other systems when classifying information. Low-sensitivity information protected by the minimum required controls in isolation must implement more restrictive controls when connected to systems containing high-sensitivity information. Information owners must consider the sensitivity of information types in the aggregate when assigning classifications. The confidentiality of an individual’s first and last name is not considered High Impact information on an isolated system. When connected to, combined with, or commingled on, a system that includes other identifiers such as a
social security number, the aggregate of the information requires classification as High Impact, highly sensitive and requires appropriate controls necessary to ensure the confidentiality of the information is maintained.

(m) **Information Sharing Agreements, Memorandums of Understanding, and Contractual Requirements** - Information Sharing Agreements, Memoranda of Understanding (MOU), grants, contracts, and other written agreements between agencies and external entities may include agreements regarding information access, sharing, use, disclosure and maintenance of information, as determined by the information classification of the information owner. The recipient organization’s information risk classification must align with any such requirements.

Additionally, if an agreement states that the recipient agency may further share the information, the subsequent recipients must adhere to the requirements of the original classification.

(n) **Intellectual Property** - Agencies must consider any intellectual property rights owned by an entity other than the State agency, when determining information risk classification assignments.

(o) **Information Lifecycle** - Agencies must consider the risk classification of information throughout its lifecycle as changes may occur prompting changes to the classification and the associated security controls. As an example, contract bids prior to award are classified as High Impact information. Post award, the risk classification of contract bids may be lowered and thus require less protective controls regarding confidentiality.

(p) **Metadata** - Agencies must consider metadata when classifying information. Metadata is often referred to as “data about data”. Metadata describes or supplements the information and may be either separate from or embedded within documents, records, or objects. Examples of metadata include filename, creation date, file size, author, etc. While metadata may not be readily readable, the sensitivity of the metadata alone or in combination with the information, needs to be considered.
APPENDIX B – GLOSSARY OF KEY TERMS

Acceptance:
The point at which the end-users of a system declare, formally, that the system meets their needs and has performed satisfactorily during the test procedures. Unless a system has been acquired, installed, or amended, purely for IT department it is not sufficient for technical staff to declare it acceptable; the end users must be involved. (SOURCE: The Information Security Glossary)

Access (Logical):
The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing an ID and password (if required). The view that restricting physical access relieves the need for logical access restrictions is misleading. Any Agency with communications links to the outside world has a security risk of logical access. (SOURCE: The Information Security Glossary)

Access:
Ability to make use of any information system (IS) resource. (SOURCE: NIST SP 800-32)

Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (SOURCE: CNSSI-4009)

Access Control:
The process of granting or denying specific requests to:
1. obtain and use information and related information processing services; and
2. enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances). (SOURCE: FIPS 201; CNSSI-4009)

Access Control List (ACL):
1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. (SOURCE: CNSSI-4009)

Access Control Mechanism:
Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. (SOURCE: CNSSI-4009)

Access Level:
A category within a given security classification limiting entry or system connectivity to only authorized persons. (SOURCE: CNSSI-4009)

Access List:
Roster of individuals authorized admittance to a controlled area. (SOURCE: CNSSI-4009)
**Access Management:**
A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data – and only using appropriate and controlled methods. Data Governance programs often focus on supporting Access Management by aligning the requirements and constraints posed by Governance, Risk Management, Compliance, Security, and Privacy efforts. (SOURCE: Data Governance Institute)

**Access Point:**
A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise network. (SOURCE: NIST SP 800-48; NIST SP 800-121)

**Access Profile:**
Association of a user with a list of protected objects the user may access. (SOURCE: CNSSI-4009)

**Account Management, User:**
Involves:
1. the process of requesting, establishing, issuing, and closing user accounts;
2. tracking users and their respective access authorizations; and
3. managing these functions.
(SOURCE: NIST SP 800-12)

**Accountability:**
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (SOURCE: NIST SP 800-27)

Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (SOURCE: CNSSI-4009)

**Activation Data:**
Private data, other than keys, that are required to access cryptographic modules.
(SOURCE: NIST SP 800-32)

**Active Attack:**
An attack that alters a system or data. (SOURCE: CNSSI-4009)

**Active Security Testing:**
Security testing that involves direct interaction with a target, such as sending packet to a target.
(SOURCE: NIST SP 800-115)

**Ad Hoc Network:**
A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station.
(SOURCE: NIST SP 800-121)
**Add-on Security:**
Incorporation of new hardware, software, or firmware safeguards in an operational information system. (SOURCE: CNSSI-4009)

**Adequate Security:**
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (SOURCE: NIST SP 800-53; FIPS 200; OMB Circular A-130, App. III)

Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Note: This includes assuring that information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls. (SOURCE: CNSSI-4009; NIST SP 800-37)

**Administrative Account:**
A user account with full privileges on a computer. (SOURCE: NIST SP 800-69)

**Administrative Safeguards:**
Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity’s workforce in relation to protecting that information. (SOURCE: NIST SP 800-66)

**Advanced Encryption Standard – (AES):**
The Advanced Encryption Standard specifies a U.S. government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. (SOURCE: FIPS 197)

A U.S. government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. (SOURCE: CNSSI-4009)

**Advanced Key Processor (AKP):**
A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to
1. exchange information with a client platform,
2. interact with fill devices, and
3. connect a client platform securely to the primary services node (PRSN). (SOURCE: CNSSI-4009)
**Advanced Persistent Threats (APT):**
An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

(i) pursues its objectives repeatedly over an extended period of time;
(ii) adapts to defenders’ efforts to resist it; and
(iii) is determined to maintain the level of interaction needed to execute its objectives.

(Source: NIST SP 800-39)

**Adversary:**
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (Source: NIST SP 800-30)

**Advisory:**
Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. (Source: CNSSI-4009)

**Affordable Care Act:**
U.S. federal statute signed into law on March 23, 2010, with the goal of expanding public and private insurance coverage and reducing the cost of healthcare for individuals and the government. (Source: IRS PUB 1075)

**Agency:**
The term “agency” is used to refer to any Department, Agency, Commission, Board, Body, or other instrumentality of the Executive Branch of New Jersey State Government.

**Agent:**
A program acting on behalf of a person or organization. (Source: NIST SP 800-95)

**Alert:**
Notification that a specific attack has been directed at an organization’s information systems. (Source: CNSSI-4009)

**Algorithm:**
A step-by-step procedure for calculations. Algorithms are used for calculation, data processing, and automated reasoning.

An algorithm is an effective method expressed as a finite list of well-defined instructions for calculating a function. Starting from an initial state and initial input (perhaps empty), the instructions describe a computation that, when executed, proceeds through a finite number of well-defined successive states, eventually producing "output" and terminating at a final ending state. The transition from one state to the next is not necessarily deterministic; some algorithms, known as randomized algorithms, incorporate random input. (Source: WIKIPEDIA)
Alternate Processing Site:
Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed. (SOURCE: ISACA)

Analysis:
The examination of acquired data for its significance and probative value to the case. (SOURCE: NIST SP 800-72)

Anomaly-Based Detection:
The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (SOURCE: NIST SP 800-94)

Anti-spoof:
Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. (SOURCE: CNSSI-4009)

Anti-Virus Software:
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. (SOURCE: NIST SP 800-83)

Antispyware Software:
A program that specializes in detecting both malware and non-malware forms of spyware. (SOURCE: NIST SP 800-69)

Applicant:
The subscriber is sometimes called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. (SOURCE: NIST SP 800-32)

Application:
A software program hosted by an information system. (SOURCE: NIST SP 800-37)

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. (SOURCE: CNSSI-4009)

Application Program Interface (API):
An API specifies how some software components should interact with each other. In addition to accessing databases or computer hardware, such as hard disk drives or video cards, an API can be used to ease the work of programming graphical user interface components. In practice, many times an API comes in the form of a library that includes specifications for routines, data structures, object classes, and variables. In some other cases, notably for SOAP and REST services, an API comes as just a specification of remote calls exposed to the API consumers. (SOURCE: WIKIPEDIA)
Application Service Providers (ASPs):
Companies that offer individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. Sometimes referred to as "apps-on-tap," ASP services are expected to become an important alternative, not only for smaller companies with low budgets for information technology, but also for larger companies as a form of outsourcing and for many services for individuals as well. Most corporations are essentially providing their own ASP service in-house, moving applications off personal computers, and putting them on a special kind of application server that is designed to handle the stripped-down kind of thin-client workstation. This allows an enterprise to reassert the central control over application cost and usage that corporations formerly had prior to the advent of the PC. (SOURCE: TechTarget)

Approval to Operate (ATO):
The official management decision issued by a DAA or PAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (SOURCE: CNSSI-4009)

Approved Mode of Operation:
A mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., Data Encryption Standard Cipher- Block Chaining (DES CBC) mode). (SOURCE: FIPS 140-2)

Approved Security Function:
A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either:
a. specified in an Approved Standard;
b. adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or
c. specified in the list of Approved security functions. (SOURCE: FIPS 140-2)

Assessment:
See Security Control Assessment.

Assessment Findings:
Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. (SOURCE: NIST SP 800-53A)

Assessment Method:
One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment. (SOURCE: NIST SP 800-53A)

Assessment Object:
The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment. (SOURCE: NIST SP 800-53A)
Assessment Procedure:
A set of assessment objectives and an associated set of assessment methods and assessment objects.
(SOURCE: NIST SP 800-53A)

Assessor:
See Security Control Assessor.

Asset:
See Information Asset.

Asset Custodian:
A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended, and that information regarding the equipment is properly documented. The asset custodian is responsible for receipt, transfer, accounting, safeguarding, and destruction of an information asset commensurate with the information’s security classification. Asset custodians have responsibility for the day-to-day operational-level functions on behalf of the information owner. Typically, asset custodians will include systems administrators, database administrators, and data managers, or other designated IT personnel. Asset custodians are responsible for supporting the information security program by:

(a) Implementing technical security controls in accordance the classification of the information and in accordance with statutory, regulatory, contractual and policy requirements
(b) Monitoring the security of the information asset and ensuring compliance with all applicable laws, regulations, contractual requirements and policies
(c) Complying with any additional security policies and procedures established by the information owner and the agency ISO
(d) Advising the information owner and the agency ISO of vulnerabilities that may present a threat to the information and of the specific means of protecting that information.
(e) Notifying the information owner and the agency ISO of any actual or attempted violations of security policies, practices, and procedures.
(f) Reporting security incidents to the NJ Cybersecurity & Communications Integration Cell (SOURCE: NJCCIC)

Asset Identification:
Security Content Automation Protocol (SCAP) constructs to uniquely identify assets (components) based on known identifiers and/or known information about the assets. (SOURCE: NIST SP 800-128)

Asset Reporting Format (ARF):
SCAP data model for expressing the transport format of information about assets (components) and the relationships between assets and reports. (SOURCE: NIST SP 800-128)
Assurance:
Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes:
1. functionality that performs correctly,
2. sufficient protection against unintentional errors (by users or software), and
3. sufficient resistance to intentional penetration or by-pass.
(SOURCE: NIST SP 800-27)

The grounds for confidence that the set of intended security controls in an information system are effective in their application. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (SOURCE: CNSSI-4009; NIST SP 800-39)

In the context of OMB M-04-04 and this document, assurance is defined as:
1. the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and
2. the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. (SOURCE: NIST SP 800-63)

Assurance Case:
A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute. (SOURCE: NIST SP 800-53A; NIST SP 800-39)

Assured Information Sharing:
The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk. (SOURCE: CNSSI-4009)

Assured Software:
Computer application that has been designed, developed, analyzed, and tested using processes, tools, and techniques that establish a level of confidence in it. (SOURCE: CNSSI-4009)

Asymmetric Cryptography:
See Public Key Cryptography. (SOURCE: CNSSI-4009)

Asymmetric Keys:
Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. (SOURCE: FIPS 201)

Asynchronous Transfer Mode (ATM):
A telecommunications concept defined by ANSI and ITU standards for carriage of a complete range of user traffic, including voice, data, and video signals. (SOURCE: WIKIPEDIA)
**Attack:**
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. (SOURCE: NIST SP 800-32)

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. (SOURCE: CNSSI-4009)

**Attack Sensing and Warning (AS&W):**
Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed. (SOURCE: CNSSI-4009)

**Attack Signature:**
A specific sequence of events indicative of an unauthorized access attempt. (SOURCE: NIST SP 800-12) A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities. (SOURCE: CNSSI-4009)

**Attribute-Based Access Control:**
Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Attribute-Based Authorization:**
A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service. (SOURCE: CNSSI-4009)

**Audit:**
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (SOURCE: NIST SP 800-32) Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. (SOURCE: CNSSI-4009)

**Audit Data:**
Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. (SOURCE: NIST SP 800-32)

**Audit Log:**
A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (SOURCE: CNSSI-4009)
Audit Reduction Tools:
Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (SOURCE: NIST SP 800-12; CNSSI-4009)

Audit Review:
The assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities, and assist in implementation of new security controls where required. This assessment is conducted annually or whenever significant change has occurred and may lead to recertification of the information system. (SOURCE: CNSSI-4009)

Audit Trail:
A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (SOURCE: NIST SP 800-47)

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. (SOURCE: CNSSI-4009)

Authenticate:
To confirm the identity of an entity when that identity is presented. (SOURCE: NIST SP 800-32)

To verify the identity of a user, user device, or other entity. (SOURCE: CNSSI-4009)

Authentication:
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; FIPS 200; NIST SP 800-30)

The process of establishing confidence of authenticity. (SOURCE: FIPS 201)

Encompasses identity verification, message origin authentication, and message content authentication. (SOURCE: FIPS 190)

A process that establishes the origin of information or determines an entity’s identity. (SOURCE: NIST SP 800-21)

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (SOURCE: CNSSI-4009)

The process of establishing confidence in the identity of users or information systems. (SOURCE: NIST SP 800-63)

Authentication Code:
A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code [MAC]). (SOURCE: FIPS 140-2)
**Authentication Mechanism:**
Hardware-or software-based mechanisms that force users to prove their identity before accessing data on a device. (SOURCE: NIST SP 800-72; NIST SP 800-124)

Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system. (SOURCE: CNSSI-4009)

**Authentication Mode:**
A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data. (SOURCE: NIST SP 800-38B)

**Authentication Period:**
The maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single terminal session or during the period data is being accessed. (SOURCE: CNSSI-4009)

**Authentication Protocol:**
A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. (SOURCE: NIST SP 800-63)

A well-specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant’s identity. (SOURCE: CNSSI-4009)

**Authentication Tag:**
A pair of bit strings associated to data to provide assurance of its authenticity. (SOURCE: NIST SP 800-38B)

**Authentication Token:**
Authentication information conveyed during an authentication exchange. (SOURCE: FIPS 196)

**Authenticator:**
The means used to confirm the identity of a user, process, or device (e.g., user password or token). (SOURCE: NIST SP 800-53; CNSSI-4009)

**Authenticity:**
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication. (SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009; NIST SP 800-39)

**Authority:**
Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere. (SOURCE: CNSSI-4009)
**Authorization:**
Access privileges granted to a user, program, or process or the act of granting those privileges. (SOURCE: CNSSI-4009)

**Authorization Boundary:**
All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

**Automated Key Transport:**
The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols). (SOURCE: FIPS 140-2)

**Automated Security Monitoring:**
Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system. (SOURCE: CNSSI-4009)

**Autonomous System (AS):**
One or more routers under a single administration operating the same routing policy. (SOURCE: NIST SP 800-54)

**Availability:**
In the context of information security, refers to ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]

Ensuring timely and reliable access to and use of information. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property of being accessible and useable upon demand by an authorized entity. (SOURCE: CNSSI-4009)

**Awareness (Information Security):**
Activities which seek to focus an individual’s attention on an (information security) issue or set of issues. (SOURCE: NIST SP 800-50)

**Backdoor:**
Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. (SOURCE: CNSSI-4009)

An undocumented way of gaining access to a computer system. A backdoor is a potential security risk. (SOURCE: NIST SP 800-82)
Bandwidth:
Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. (SOURCE: Safety Engineering: Principles and Practices)

Banner:
The information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use. (SOURCE: Intrusion Detection Systems)

Banner Grabbing:
The process of capturing banner information—such as application type and version—that is transmitted by a remote port when a connection is initiated. (SOURCE: NIST SP 800-115)

Baseline:
Hardware, software, databases, and relevant documentation for an information system at a given point in time. (SOURCE: CNSSI-4009)

Baseline Assessment:
An interim compliance validation assessment performed by a QSA to determine the PCI Security compliance status. (SOURCE: VERIZON PCI SECURITY)

Baseline Configuration:
A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. (SOURCE: NIST SP 800-128)

Baseline Security:
The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection. (SOURCE: NIST SP 800-16)

Baselining:
Monitoring resources to determine typical utilization patterns so that significant deviations can be detected. (SOURCE: NIST SP 800-61)

Basic Testing:
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing. (SOURCE: NIST SP 800-53A)

Bastion Host:
A special-purpose computer on a network specifically designed and configured to withstand attacks. (SOURCE: CNSSI-4009)

Best Practice:
A proven activity or process that has been successfully used by multiple enterprises. (SOURCE: ISACA)
**Binding:**
Process of associating two related elements of information. (SOURCE: NIST SP 800-32)

An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through:
1. a certification authority’s generation of a public key certificate,
2. a security officer’s verification of an entity’s credentials and placement of the entity’s public key and identifier in a secure database, or
3. an analogous method.
(SOURCE: NIST SP 800-21)

Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. (SOURCE: CNSSI-4009)

**Biometric:**
A physical or behavioral characteristic of a human being. (SOURCE: NIST SP 800-32)

A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (SOURCE: FIPS 201)

**Biometric Information:**
The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns.) (SOURCE: FIPS 201)

**Biometric System:**
An automated system capable of: 1) capturing a biometric sample from an end user; 2) extracting biometric data from that sample; 3) comparing the extracted biometric data with data contained in one or more references; 4) deciding how well they match; and 5) indicating whether or not an identification or verification of identity has been achieved.
(SOURCE: FIPS 201)

**Biometrics:**
Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (SOURCE: CNSSI-4009)

**Black Box Testing:**
See Basic Testing.

**Blacklist:**
A list of email senders who have previously sent spam to a user. (SOURCE: NIST SP 800-114)

A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. (SOURCE: NIST SP 800-94)
**Blacklisting:**
The process of the system invalidating a user ID based on the user’s inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources. (SOURCE: CNSSI-4009)

**Blended Attack:**
A hostile action to spread malicious code via multiple methods. (SOURCE: CNSSI-4009)

**Blinding:**
Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a “real” attack performed simultaneously. (SOURCE: NIST SP 800-94)

**Block:**
Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes. (SOURCE: FIPS 197)

**Block Cipher:**
A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block. (SOURCE: NIST SP 800-90)

**Block Cipher Algorithm:**
A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length. (SOURCE: NIST SP 800-67)

**Blog:**
A discussion or informational site published on the World Wide Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). Blogs may be the work of a single individual, occasionally of a small group, and covering a single subject, or may include posts written by large numbers of authors and professionally edited. (SOURCE: WIKIPEDIA)

**Body of Evidence (BoE):**
The set of data that documents the information system’s adherence to the security controls applied. The BoE will include a Requirements Verification Traceability Matrix (RVTM) delineating where the selected security controls are met and evidence to that fact can be found. The BoE content required by an Authorizing Official will be adjusted according to the impact levels selected. (SOURCE: CNSSI-4009)

**Border Gateway Protocol (BGP):**
A standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol, but is sometimes also classed as a distance vector routing protocol. The Border Gateway Protocol does not use Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on paths, network policies and/or rule-sets configured by a network administrator. The Border Gateway Protocol plays a key role in the overall operation of the Internet and is involved in making core routing decisions. (SOURCE: WIKIPEDIA)
**Boundary Protection:**
Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
(SOURCE: NIST SP 800-53; CNSSI-4009)

**Boundary Protection Device:**
A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection. (SOURCE: NIST SP 800-53)

A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems. (SOURCE: CNSSI-4009)

**Breach:**
An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.
(SOURCE: HIPAA (45 CFR §§ 164.400-414)

**Beach of Security:**
"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. (SOURCE: N.J.S.A 2C.56:8-161)

**Bring Your Own Device (BYOD):**
Refers to the policy of permitting employees and contractors to use personally owned or third-party owned mobile devices (e.g. tablets, and smart phones) for State business purposes.

**Brute Force Password Attack:**
A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. (SOURCE: NIST SP 800-72)
Buffer Overflow:
A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. (SOURCE: NIST SP 800-28; CNSSI-4009)

Bulk Encryption:
Simultaneous encryption of all channels of a multichannel telecommunications link. (SOURCE: CNSSI-4009)

Business Associate:
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (SOURCE: US Department of Health and Human Services)

Business Continuity Plan (BCP):
The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption. (SOURCE: NIST SP 800-34; CNSSI-4009)

Business Entity:
All trusted Entities that are authorized and/or contracted with a Department and/or Agency within the Executive Branch of State Government for the purpose of this policy Business Entity may include other governmental agencies outside the Executive Branch that do not make use of the Garden State Network. (SOURCE: NJOIT Glossary)

Business Impact Analysis (BIA):
An analysis of an information system’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (SOURCE: NIST SP 800-34)

An analysis of an enterprise’s requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. (SOURCE: CNSSI-4009)

Call Back:
Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact. (SOURCE: CNSSI-4009)

Card Skimmer:
A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card. (SOURCE: PCI DSS GLOSSARY)
Card Verification Value (CVV/CVV2):
Both of these terms are commonly used to refer to the number printed on a card to help secure "card not present" transactions - other terms include CVC, CID and CSC. To be precise, the code printed on the card is actually the CVV2 - and the CVV is integrity-check data encoded on the magnetic strip - but both terms are widely used online. (SOURCE: VERIZON PCI SECURITY)

Cardholder:
An individual possessing an issued Personal Identity Verification (PIV) card. (SOURCE: FIPS 201)

Cardholder Data Environment (CDE):
All people, processes and technologies that store, process or transmit cardholder data (CHD) or sensitive authentication data (SAD). (SOURCE: VERIZON PCI SECURITY)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):
A media access control method used most notably in local area networking. It uses a carrier sensing scheme in which a transmitting data station detects other signals while transmitting a frame, and stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame. (SOURCE: WIKIPEDIA)

Category:
Restrictive label applied to classified or unclassified information to limit access. (SOURCE: CNSSI-4009)

Certificate:
A digital representation of information which at least
1. identifies the certification authority issuing it,
2. names or identifies its subscriber,
3. contains the subscriber’s public key,
4. identifies its operational period, and
5. is digitally signed by the certification authority issuing it.
(SOURCE: NIST SP 800-32)

A set of data that uniquely identifies an entity, contains the entity’s public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its crypto period. (SOURCE: NIST SP 800-21)

A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair. The certificate contains the owner’s public key and possibly other information, and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner. (SOURCE: FIPS 186)

Certificate Management:
Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (SOURCE: CNSSI-4009)

Certificate Management Authority – (CMA):
A Certification Authority (CA) or a Registration Authority (RA). (SOURCE: NIST SP 800-32)
Certificate of Authority:
In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard. (SOURCE: Wikipedia)

Certificate Policy (CP):
A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (SOURCE: CNSSI-4009; NIST SP 800-32)

Certificate Revocation List (CRL):
A list of revoked public key certificates created and digitally signed by a Certification Authority. (SOURCE: NIST SP 800-63; FIPS 201)

Certification:
A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: FIPS 200)

The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. (SOURCE: FIPS 201)

Comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See Security Control Assessment. (SOURCE: CNSSI-4009)

Certification Authority (CA):
A trusted entity that issues and revokes public key certificates. (SOURCE: FIPS 201)

The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy. (SOURCE: NIST SP 800-21; FIPS 186)

Certification Authority Facility:
The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. (SOURCE: NIST SP 800-32)
**Certification Package:**
Product of the certification effort documenting the detailed results of the certification activities. (SOURCE: CNSSI-4009)

**Chain of Custody:**
A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (SOURCE: NIST SP 800-72; CNSSI-4009)

**Chain of Evidence:**
A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. (SOURCE: CNSSI-4009)

**Change:**
The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items. (SOURCE: ITIL V3)

**Change Control:**
A formal process used to ensure that a process, product, service, or technology component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data Governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data. (SOURCE: Data Governance Institute)

**Change Control Board (CCB):**
A committee that makes decisions regarding whether or not proposed changes to a software project should be implemented. In short any changes to the Baseline Requirements agreed with the client, should be taken up by project team on approval from this committee. If any change is agreed by the committee, it is communicated to the project team and client and the requirement is Baselined with the change. The change control board is constituted of project stakeholders or their representatives. The authority of the change control board may vary from project to project, but decisions reached by the change control board are often accepted as final and binding. The decision of acceptance of the changes also depends upon the stage or phase of the project. The main objective is to ensure acceptance of the project (deliverable) by the client. (SOURCE: WIKIPEDIA)

**Check Word:**
Cipher text generated by cryptographic logic to detect failures in cryptography. (SOURCE: CNSSI-4009)

**Checksum:**
Value computed on data to detect error or manipulation. (SOURCE: CNSSI-4009)
**Cipher:**
Series of transformations that converts plaintext to ciphertext using the Cipher Key. (SOURCE: FIPS 197)

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both. (SOURCE: CNSSI-4009)

**Cipher Block Chaining-Message Authentication Code – (CBC-MAC):**
A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic. (SOURCE: NIST SP 800-38C)

**Cipher Suite:**
Negotiated algorithm identifiers. Cipher suites are identified in human-readable form using a pneumatic code. (SOURCE: NIST SP 800-52)

**Cipher Text Auto-Key (CTAK):**
Cryptographic logic that uses previous cipher text to generate a key stream. (SOURCE: CNSSI-4009)

**Ciphertext:**
Data output from the Cipher or input to the Inverse Cipher. (SOURCE: FIPS 197)

Data in its enciphered form. (SOURCE: NIST SP 800-56B)

**Claimant:**
A party whose identity is to be verified using an authentication protocol. (SOURCE: NIST SP 800-63; FIPS 201)

An entity that is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard [claimant] can act on behalf of a human user [principal]). (SOURCE: FIPS 196)

An entity (user, device or process) whose assertion is to be verified using an authentication protocol. (SOURCE: CNSSI-4009)

**Clear:**
To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on Clear/Purge Convergence. (SOURCE: NIST SP 800-88)

**Clear Text:**
Information that is not encrypted. (SOURCE: NIST SP 800-82)
Clearing:
Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods. (SOURCE: CNSSI-4009)

Client:
A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server. (SOURCE: NIST SP 800-32)

Closed Security Environment:
Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control. (SOURCE: CNSSI-4009)

Cloud Access Security Broker (CASB):
On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention. (SOURCE: Gartner)

Cloud Computing:
A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Note: Both the user's data and essential security services may reside in and be managed within the network cloud. (SOURCE: CNSSI-4009)

CloudConnect:
A bundled offering of cloud-based Microsoft Office365 products, including email, instant messaging, video conferencing, file sharing, and storage. It enables user-friendly interagency communication and file sharing, multi-device content synchronization, and two-factor authenticated remote access. (SOURCE: State of New Jersey Statewide Information Security Manual)
Cloud Service Provider:
An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, such as NJOIT, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

Cold Site:
Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services. (SOURCE: CNSSI-4009)

A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. (SOURCE: NIST SP 800-34)

Cold Start:
Procedure for initially keying crypto-equipment. (SOURCE: CNSSI-4009)

Collision:
Two or more distinct inputs produce the same output. Also see Hash Function.
(SOURCE: NIST SP 800-57 Part 1)

Comingling:
The presence of FTI and non-FTI data together on the same paper or electronic media.
(SOURCE: IRS PUB 1075)

Common Configuration Enumeration (CCE):
A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products. (SOURCE: NIST SP 800-128)

Common Configuration Scoring System (CCSS):
A set of measures of the severity of software security configuration issues. (SOURCE: NISTIR 7502)

A SCAP specification for measuring the severity of software security configuration issues.
(SOURCE: NIST SP 800-128)

Common Platform Enumeration (CPE):
A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type. (SOURCE: NIST SP 800-128)
Common Vulnerabilities and Exposures (CVE):
A dictionary of common names for publicly known information system vulnerabilities.
(SOURCE: NIST SP 800-51; CNSSI-4009)

An SCAP specification that provides unique, common names for publicly known information system vulnerabilities. (SOURCE: NIST SP 800-128)

Common Vulnerability Scoring System (CVSS):
An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity. (SOURCE: NIST SP 800-128)

Communications Security (COMSEC):
A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material. (SOURCE: CNSSI-4009)

Comparison:
The process of comparing a biometric with a previously stored reference. (SOURCE: FIPS 201)

Compensating Security Control:
A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
(SOURCE: CNSSI-4009)

Compliance:
A discipline, set of practices, and/or organizational group that deals with adhering to laws, regulations, standards, and contractual arrangements. Also, the adherence to requirements. Data Governance programs often support many types of compliance requirements: Regulatory compliance, contractual compliance, adherence to internal standards, policies, and architectures, and conformance to rules for data management, project management, and other disciplines. (SOURCE: Data Governance Institute)

Comprehensive Testing:
A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.
(SOURCE: NIST SP 800-53A)

Compromise:
Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (SOURCE: NIST SP 800-32; CNSSI-4009)

The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). (SOURCE: FIPS 140-2)
**Computer-Based Training:**
Computer-based training (CBT) is any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through a corporate or educational intranet, or over the Internet as Web-based training (SOURCE: TechTarget)

**Computer Cryptography:**
Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. (SOURCE: CNSSI-4009)

**Computer Emergency Response Team (CERT):**
Acronym for Carnegie Mellon University’s "Computer Emergency Response Team." The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services. (SOURCE: PCI DSS GLOSSARY)

**Computer Incident Response Team (CIRT):**
Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team). (SOURCE: CNSSI-4009)

**Computer Network Attack (CNA):**
Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (SOURCE: CNSSI-4009)

**Computer Network Defense (CND):**
Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (SOURCE: CNSSI-4009)

**Computer Network Exploitation (CNE):**
Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks. (SOURCE: CNSSI-4009)

**Computer Security (COMPUSEC):**
Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (SOURCE: CNSSI-4009)

**Computer Security Incident:**
See incident.
**Computer Security Incident Response Team (CSIRT):**
A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). (SOURCE: NIST SP 800-61)

**Computer Security Object (CSO):**
A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

**Computer Security Objects Register:**
A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

**Computer Security Objects Register:**
A collection of Computer Security Object names and definitions kept by a registration authority. (SOURCE: FIPS 188; CNSSI-4009)

**Confidentiality:**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. (SOURCE: FIPS 140-2)

The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (SOURCE: CNSSI-4009)

**Configuration Control:**
Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. (SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53)

**Configuration Item:**
Any component or other service asset that needs to be managed in order to deliver an IT service. (SOURCE: ITIL V3)

**Configuration Management:**
A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle. (SOURCE: IRS PUB 1075)

**Container:**
The file used by a virtual disk encryption technology to encompass and protect other files. (SOURCE: NIST SP 800-111)
**Contamination:**
Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. (SOURCE: CNSSI-4009)

**Content Filtering:**
The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. (SOURCE: NIST SP 800-114)

**Contingency Plan:**
Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. (SOURCE: CNSSI-4009)

**Continuity of Operations (COOP) Plan:**
A predetermined set of instructions or procedures that describe how an organization’s mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (SOURCE: NIST SP 800-34)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan. (SOURCE: CNSSI-4009)

**Continuous Monitoring:**
The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes:

1. The development of a strategy to regularly evaluate selected IA controls/metrics,
2. Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events,
3. Recording changes to IA controls, or changes that affect IA risks, and
4. Publishing the current security status to enable information-sharing decisions involving the enterprise.

(SOURCE: CNSSI-4009)

Maintaining ongoing awareness to support organizational risk decisions. (SOURCE: NIST SP 800-137)
Control:
A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activates. They can include actions, devices, procedures, techniques, or other measures. (SOURCE: Data Governance Institute)

Control Information:
Information that is entered into a cryptographic module for the purposes of directing the operation of the module. (SOURCE: FIPS 140-2)

Controlled Access Area:
Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance. (SOURCE: CNSSI-4009)

Controlled Area:
Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. (SOURCE: NIST SP 800-53)

Controlled Interface:
A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. (SOURCE: CNSSI-4009; NIST SP 800-37)

Cookie:
A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (SOURCE: NIST SP 800-28)

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. (SOURCE: CNSSI-4009)

Corrective Action Plan (CAP):
A report required to be filed semi-annually, detailing the agency’s planned and completed actions to resolve findings identified during an IRS safeguard review. (SOURCE: IRS PUB 1075)

Countermeasures:
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200)

Covert Testing:
Testing performed using covert methods and without the knowledge of the organization’s IT staff, but with the full knowledge and permission of upper management. (SOURCE: NIST SP 800-115)
Credential:
An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (SOURCE: NIST SP 800-63)

Evidence attesting to one’s right to credit or authority. (SOURCE: FIPS 201)

Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once. (SOURCE: CNSSI-4009)

Criminal Justice Information (CJI):
Criminal Justice Information is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to: biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, it can include: fingerprints, palm prints, iris scans, and facial recognition data.
- Identity History Data - textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data - information about vehicles and property associated with a crime when accompanied by any personally identifiable information (PII).
- Case/Incident History - information about the history of criminal incidents.

(SOURCE: FBI)

Crisis Management Plan (CMP):
Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms. Communication that occurs within the response phase of emergency-management scenarios. Crisis-management methods of a business or an organization are called a crisis-management plan. (SOURCE: WIKIPEDIA)

Critical Infrastructure:
System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] (SOURCE: CNSSI-4009)

Criticality:
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (SOURCE: NIST SP 800-60)
Cross-Site Scripting (XSS):
Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection. (SOURCE: PCI DSS GLOSSARY)

Cryptographic Algorithm:
A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (SOURCE: NIST SP 800-21; CNSSI-4009)

Cryptographic Hash Function:
A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
1. (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and
2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
(SOURCE: NIST SP 800-21)

Cryptographic Key:
A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A binary string used as a secret parameter by a cryptographic algorithm. (SOURCE: NIST SP 800-108)

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. (SOURCE: FIPS 201; FIPS 198)

A parameter used in conjunction with a cryptographic algorithm that determines
- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- A digital signature computed from data,
- The verification of a digital signature computed from data,
- An authentication code computed from data, or
- An exchange agreement of a shared secret.
(SOURCE: FIPS 140-2)

Cryptographic Token:
A token where the secret is a cryptographic key. (SOURCE: NIST SP 800-63)

A portable, user-controlled physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions. (SOURCE: CNSSI-4009)
**Cryptography:**
The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (SOURCE: NIST SP 800-59)

The discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (SOURCE: NIST SP 800-21)

Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography that makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret. (SOURCE: FIPS 191)

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (SOURCE: CNSSI-4009)

**Cryptology:**
The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (SOURCE: NIST SP 800-60)

The mathematical science that deals with cryptanalysis and cryptography. (SOURCE: CNSSI-4009)

**Cyber Attack:**
An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (SOURCE: CNSSI-4009)

**Cyber Incident:**
Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident. (SOURCE: CNSSI-4009)

**Cyber Infrastructure:**
Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure. (SOURCE: NISTIR 7628)
Cybersecurity:
The ability to protect or defend the use of cyberspace from cyberattacks. (SOURCE: CNSSI-4009)

The process of protecting information by preventing, detecting, and responding to attacks. (SOURCE: NIST CYBERSECURITY FRAMEWORK)

Cybersecurity Event:
A change that may have an impact on organizational operations (including mission, capabilities, or reputation). (SOURCE: NIST CYBERSECURITY FRAMEWORK)

Cyberspace:
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (SOURCE: CNSSI-4009)

Cyclical Redundancy Check (CRC):
A method to ensure data has not been altered after being sent through a communication channel. (SOURCE: NIST SP 800-72)

Error checking mechanism that verifies data integrity by computing a polynomial algorithm based checksum. (SOURCE: CNSSI-4009)

Data:
A subset of information in an electronic format that allows it to be retrieved or transmitted. (SOURCE: CNSSI-4009)

Data Asset:
1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.

Data Custodian:
Anyone with physical or operational control of a data repository, including, without limitation, roles such as database administrators, system or server administrators, backup operators and storage server administrators. (SOURCE: Data Governance Institute)

Data Encryption Standard (DES):
The DEA cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (SOURCE: NIST SP 800-67)
**Data Governance:**
The exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets. (SOURCE: DAMA DMBOK)

A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models, which describe who can take what actions with what information, and when, under what circumstances, using what methods. (SOURCE: Data Governance Institute)

**Data Integrity:**
The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (SOURCE: CNSSI-4009)

**Data Loss:**
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (SOURCE: NIST SP 800-137)

**Data Loss Prevention (DLP):**
A system that restricts the transmission of sensitive data, reducing the risk of suffering a breach. (SOURCE: VERIZON PCI SECURITY)

**Data Privacy:**
The assurance that a person’s or organization’s personal and private information is not inappropriately disclosed. Ensuring Data Privacy requires Access Management, eSecurity, and other data protection efforts. (SOURCE: Data Governance Institute)

**Data Security:**
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (SOURCE: CNSSI-4009)

**Decertification:**
Revocation of the certification of an information system item or equipment for cause. (SOURCE: CNSSI-4009)

**Decrypt:**
Generic term encompassing decode and decipher. (SOURCE: CNSSI-4009)
**Decryption:**
The process of transforming ciphertext into plaintext. (SOURCE: NIST SP 800-67)

The process of changing ciphertext into plaintext using a cryptographic algorithm and key. (SOURCE: NIST SP 800-21)

Conversion of ciphertext to plaintext through the use of a cryptographic algorithm. (SOURCE: FIPS 185)

**Dedicated Mode:**
Information systems security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:
1. valid security clearance for all information within the system,
2. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and
3. valid need-to-know for all information contained within the information system. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (SOURCE: CNSSI-4009)

**Default Classification:**
Classification reflecting the highest classification being processed in an information system. Default classification is included in the caution statement affixed to an object. (SOURCE: CNSSI-4009)

**Defense-in-Breadth:**
A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (SOURCE: CNSSI-4009; NIST SP 800-53)

**Defense-in-Depth:**
Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. (SOURCE: CNSSI-4009; NIST SP 800-53)

**Degauss:**
Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. (SOURCE: CNSSI-4009)

**Deleted File:**
A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data. (SOURCE: NIST SP 800-72)
Demilitarized Zone (DMZ):
An interface on a routing firewall that is similar to the interfaces found on the firewall’s protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (SOURCE: NIST SP 800-41)

A host or network segment inserted as a "neutral zone" between an organization’s private network and the Internet. (SOURCE: NIST SP 800-45)

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network’s Information Assurance policy for external information exchange and to provide external, untrusted (SOURCEs with restricted access to releasable information while shielding the internal networks from outside attacks. (SOURCE: CNSSI-4009)

Denial of Service (DoS):
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) (SOURCE: CNSSI-4009)

Deny by Default / Allow by Exception:
A firewall configuration policy that forces the user to register at the site, authenticate and authorize prior to gaining access. (SOURCE: SECUROSIS WEBSITE)

Depth:
An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive. (SOURCE: NIST SP 800-53A)

Digital Evidence:
Electronic information stored or transferred in digital form. (SOURCE: NIST SP 800-72)

Digital Forensics:
The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (SOURCE: NIST SP 800-86)
Digital Signature:
An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. (SOURCE: NIST SP 800-63)

A non-forgable transformation of data that allows the proof of the (SOURCE (with non-repudiation) and the verification of the integrity of that data. (SOURCE: FIPS 196)

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:
1. origin authentication,
2. data integrity, and
3. signer non-repudiation.
(SOURCE: FIPS 140-2)

The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation. (SOURCE: FIPS 186-3)

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, data integrity, and signatory non-repudiation. (SOURCE: NIST SP 800-89)

Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay. (SOURCE: CNSSI-4009)

Digital Signing:
An attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users’ private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the ‘digitally signed’ document) that can only be decrypted by applying the user’s public key. (Also digitally signing, digital signature)

Direct-Attached Storage (DAS):
A digital storage system directly attached to a server or workstation, without a storage network in between. (SOURCE: WIKIPEDIA)

Disaster Recovery Plan (DRP):
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. (SOURCE: NIST SP 800-34)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days.

**Discretionary Access Control:**
The basis of this kind of security is that an individual user, or program operating on the user’s behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user’s control. (SOURCE: FIPS 191)

A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (SOURCE: CNSSI-4009)

**Disruption:**
An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: CNSSI-4009)

An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: NIST SP 800-34)

**Distributed Denial of Service – (DDoS):**
A Denial of Service technique that uses numerous hosts to perform the attack. (SOURCE: CNSSI-4009)

**Domain:**
A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-37)

**Domain Name System (DNS):**
A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985. (SOURCE: Wikipedia)

**Dynamic Host Configuration Protocol (DHCP):**
A standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually. (SOURCE: WIKIPEDIA)
**Eavesdropping Attack:**
An attack in which an Attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the Claimant.  
(SOURCE: NIST SP 800-63)

**Egress Filtering:**
Filtering of outgoing network traffic. (SOURCE: NIST SP 800-41)

**Electronic Authentication (E-authentication):**
The process of establishing confidence in user identities electronically presented to an information system. (SOURCE: NIST SP 800-63; CNSSI-4009)

**Electronic Key Entry:**
The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.) (SOURCE: FIPS 140-2)

**Electronic Key Management System (EKMS):**
Interoperable collection of systems being developed by services and agencies of the U.S. government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material. (SOURCE: CNSSI-4009)

**Electronic Messaging Services:**
Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business. (SOURCE: CNSSI-4009)

**Electronic Signature:**
The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature. (SOURCE: CNSSI-4009)

**Embedded Cryptographic System:**
Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. (SOURCE: CNSSI-4009)

**Embedded Cryptography:**
Cryptography engineered into an equipment or system whose basic function is not cryptographic. (SOURCE: CNSSI-4009)

**Embedded System:**
An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Some examples of embedded systems include ATMs, cell phones, printers, thermostats, calculators, and videogame consoles. (SOURCE: Wikipedia)
**Embedded Technology:**
Specialized hardware and software that is wholly incorporated as part of a larger system or machine.  
(SOURCE: Army Knowledge Management and Information Technology)

**Encode:**
Convert plain text to cipher text by means of a code.  
(SOURCE: CNSSI-4009)

**Encrypt:**
Generic term encompassing encipher and encode.  
(SOURCE: CNSSI-4009)

**Encrypted Key:**
A cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.  
(SOURCE: FIPS 140-2)

**Encrypted Network:**
A network on which messages are encrypted (e.g., using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.  
(SOURCE: NIST SP 800-32)

**Encryption:**
Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.  
(SOURCE: FIPS 185)

The process of changing plaintext into ciphertext for the purpose of security or privacy.  
(SOURCE: NIST SP 800-21; CNSSI-4009)

**Encryption Algorithm:**
Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.  
(SOURCE: CNSSI-4009)

**Encryption Certificate:**
A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.  
(SOURCE: NIST SP 800-32)

**End-to-End Encryption:**
Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.  
(SOURCE: NIST SP 800-12)

Encryption of information at its origin and decryption at its intended destination without intermediate decryption.  
(SOURCE: CNSSI-4009)

**End-to-End Security:**
Safeguarding information in an information system from point of origin to point of destination.  
(SOURCE: CNSSI-4009)
Endpoint:
Any device capable of being connected, either physically or wirelessly to a network and accepts communications back and forth across the network. Endpoints include, but are not limited to, computers, servers, tablets, mobile devices, or any similar network enabled device. (SOURCE: NJCCIC)

Enterprise:
An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (SOURCE: CNSSI-4009)

Enterprise Architecture (EA):
The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture. (SOURCE: CNSSI-4009)

Enterprise Risk Management:
The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary. (SOURCE: CNSSI-40)

Entity:
Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). (SOURCE: NIST SP 800-27)

An active element in an open system. (SOURCE: FIPS 188)

Any participant in an authentication exchange; such a participant may be human or nonhuman, and may take the role of a claimant and/or verifier. (SOURCE: FIPS 196)

Entrapment:
Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations. (SOURCE: CNSSI-4009)

Entropy:
A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. (SOURCE: NIST SP 800-63)

Environment:
Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. (SOURCE: FIPS 200; CNSSI-4009)
Erasure:
Process intended to render magnetically stored information irretrievable by normal means. (SOURCE: CNSSI-4009)

Error Detection Code:
A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. (SOURCE: FIPS 140-2; CNSSI-4009)

Escrow:
Something (e.g., a document, an encryption key) that is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition." (SOURCE: FIPS 185)

Event:
Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. (SOURCE: CNSSI-4009; NIST SP 800-61)

Examination:
A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data. (SOURCE: NIST SP 800-72)

Examine:
A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

Exculpatory Evidence:
Evidence that tends to decrease the likelihood of fault or guilt. (SOURCE: NIST SP 800-72)

Expected Output:
Any data collected from monitoring and assessments as part of the Information Security Continuous Monitoring (ISCM) strategy. (SOURCE: NIST SP 800-137)

Exploit Code:
A program that allows attackers to automatically break into a system. (SOURCE: NIST SP 800-40)

External Information System (or Component):
An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-40)
**External Information System Service Provider:**
A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (SOURCE: NIST SP 800-37; NIST SP 800-53)

**External Network:**
A network not controlled by the organization. (SOURCE: NIST SP 800-53; CNSSI-4009)

**External Party:**
A person external to New Jersey State Government.

**External Security Testing:**
Security testing conducted from outside the organization’s security perimeter. (SOURCE: NIST SP 800-115)

**Extranet:**
A private network that uses Web technology, permitting the sharing of portions of an enterprise’s information or operations with suppliers, vendors, partners, customers, or other enterprises. (SOURCE: CNSSI-4009)

**Failover:**
The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Failure Access:**
Type of incident in which unauthorized access to data results from hardware or software failure. (SOURCE: CNSSI-4009)

**Failure Control:**
Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery. (SOURCE: CNSSI-4009)
**False Acceptance:**
When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. (SOURCE: NIST SP 800-76)

In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. (SOURCE: CNSSI-4009)

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. (SOURCE: NIST SP 800-76)

The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system’s false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. (SOURCE: CNSSI-4009)

**False Positive:**
An alert that incorrectly indicates that malicious activity is occurring. (SOURCE: NIST SP 800-61)

**Federal Identity, Credentials, and Access Management (FICAM):**
The programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and NPEs, bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. ICAM cuts across numerous offices, programs, and systems within an agency’s enterprise, which are typically directed and managed separately. As a result, many of the aspects of ICAM within the Federal Government have traditionally been managed within individual stove-pipes. The following figure provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stove-pipes can intersect to provide an enterprise capability. (SOURCE: FICAM ROADMAP AND IMPLEMENTATION GUIDANCE)

**Federal Information Processing Standard (FIPS):**
A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. (SOURCE: FIPS 201)
Federal Information Security Management Act (FISMA):  
A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB. (SOURCE: CNSSI-4009)

Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided. (SOURCE: NIST SP 800-63)

Federal Risk and Authorization Management Program (FedRAMP):  
A federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. (SOURCE: http://cloud.cio.gov/fedramp)

Federal Tax Information (FTI) – Federal Tax information consists of federal tax returns and return information (and information derived from it) that is in the agency’s possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(b) agreement. FTI includes any information created by the recipient that is derived from Federal return or return information received from the IRS or obtained through a secondary source. (SOURCE: IRS).

File Encryption:  
The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. (SOURCE: NIST SP 800-111)

File Protection:  
Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents. (SOURCE: CNSSI-4009)

File Security:  
Means by which access to computer files is limited to authorized users only. (SOURCE: CNSSI-4009)

File Transfer Protocol (FTP):  
Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. (SOURCE: PCI DSS GLOSSARY)
Firewall:
A gateway that limits access between networks in accordance with local security policy.
(SOURCE: NIST SP 800-32)

A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. (SOURCE: CNSSI-4009)

A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. (SOURCE: NIST SP 800-41)

Firewall Control Proxy:
The component that controls a firewall’s handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination. (SOURCE: NIST SP 800-58)

Firmware:
The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
(SOURCE: FIPS 140-2)

Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. (SOURCE: CNSSI-4009)

Flash:
A multimedia and software platform used for creating vector graphics, animation, games and rich Internet applications (RIAs) that can be viewed, played and executed in Adobe Flash Player. Flash is frequently used to add streamed video or audio players, advertisement and interactive multimedia content to web pages. (SOURCE: WIKIPEDIA)

Flaw:
Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. (SOURCE: CNSSI-4009)

Flooding:
An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (SOURCE: CNSSI-4009)

Forensics:
The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (SOURCE: CNSSI-4009)

Frame Relay:
A standardized wide area network (WAN) technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces. (SOURCE: WIKIPEDIA)
Full Disk Encryption (FDE):
The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer’s operating system, and permitting access to the data only after successful authentication with the full disk encryption product. (SOURCE: NIST SP 800-111)

Function:
A team or group of people and the tools or other resources they use to carry out one or more processes or activities. (SOURCE: ITIL V3)

Functional Testing:
Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. (SOURCE: CNSSI-4009)

Gateway:
Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. (SOURCE: CNSSI-4009)

Gateways:
Points (network point, device, software, etc.) that act as an entrance to another point (network, computer, software application, etc.).

Governance:
Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. (SOURCE: ISACA)

Governance, Risk, and Compliance (GRC):
Governance, Risk, and Compliance is a term often used by management to acknowledge the interdependencies of these three disciplines in setting policy. See also GRC-SQ and Risk Management. (SOURCE: Data Governance Institute)

Group Authenticator:
Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group. (SOURCE: CNSSI-4009)

Hacker:
Unauthorized user who attempts to or gains access to an information system. (SOURCE: CNSSI-4009)

Handshaking Procedures:
Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another. (SOURCE: CNSSI-4009)
Hash Value:
The result of applying a cryptographic hash function to data (e.g., a message). (SOURCE: NIST SP 800-106)

Hashing:
The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. (SOURCE: NIST SP 800-72; CNSSI-4009)

Health information:
means any information, whether oral or recorded in any form or medium, that:

(a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(SOURCE: HIPAA)

High Availability:
A failover feature to ensure availability during device or component interruptions. (SOURCE: NIST SP 800-113)

High Impact:
The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e.,

5. causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

6. results in major damage to organizational assets;

7. results in major financial loss; or

8. results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).

(SOURCE: FIPS 199; CNSSI-400)

High-Impact System:
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200)

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high. (SOURCE: CNSSI-4009)
**HIPAA:**
The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. (SOURCE: WIKIPEDIA)

**HITECH:**
The Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5). Under the HITECH Act, the United States Department of Health and Human Services is spending $25.9 billion to promote and expand the adoption of health information technology. (SOURCE: WIKIPEDIA)

**Honeypot:**
A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. (SOURCE: CNSSI-4009)

**Host:**
A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services. (SOURCE: IRS PUB 1075)

**Hot Site:**
A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption. (SOURCE: NIST SP 800-34)

Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization. (SOURCE: CNSSI-4009)

**Hybrid Security Control:**
A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See also Common Control and System-Specific Security Control. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)
**Hypertext Transfer Protocol (HTTP):**
An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext. (SOURCE: WIKIPEDIA)

**Hypertext Transfer Protocol Over Secure Socket Layer (HTTPS):**
Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins. (SOURCE: PCI GLOSSARY)

**Hypervisor:**
Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM). (SOURCE: PCI DSS GLOSSARY)

**Identification:**
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (SOURCE: NIST SP 800-47)

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (SOURCE: FIPS 201)

An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. (SOURCE: CNSSI-4009)

**Identifier:**
Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers. (SOURCE: FIPS 201)

A data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others. (SOURCE: CNSSI-4009)

**Identity:**
A set of attributes that uniquely describe a person within a given context. (SOURCE: NIST SP 800-63)

The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (SOURCE: FIPS 201)

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager’s responsibility, is sufficient to distinguish that entity from any other entity. (SOURCE: CNSSI-4009)
Identity Proofing:
The process by which a Credentials Service Provider (CSP) and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. (SOURCE: NIST SP 800-63)

The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity. (SOURCE: FIPS 201)

Identity Registration:
The process of making a person’s identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person’s relevant attributes into the system. (SOURCE: FIPS 201; CNSSI-4009)

Identity Token:
Smart card, metal key, or other physical object used to authenticate identity. (SOURCE: CNSSI-4009)

Identity Validation:
Tests enabling an information system to authenticate users or resources. (SOURCE: CNSSI-4009)

Identity Verification:
The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card of system and associated with the identity being claimed. (SOURCE: FIPS 201; NIST SP 800-79)

Identity-Based Access Control:
Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (SOURCE: NIST SP 800-53; CNSSI-4009)

Identity-Based Security Policy:
A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access. (SOURCE: NIST SP 800-33)
**Individually Identifiable Health Information:**
Information that is a subset of health information, including demographic information collected from an individual, and:

(a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(SOURCE: HIPAA)

**Impact:**
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: NIST SP 800-60)

**Impact Level:**
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: CNSSI-4009)

High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized. (SOURCE: NIST SP 800-34)

**Inadvertent Disclosure:**
Type of incident involving accidental exposure of information to an individual not authorized access. (SOURCE: CNSSI-4009)

**Incident (ITIL):**
An unplanned interruption to an IT service, or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident. (SOURCE: ITIL V3 SERVICE OPERATION 7.2.2)

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (SOURCE: NIST SP 800-61)

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (SOURCE: FIPS 200; NIST SP 800-53)
An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (SOURCE: CNSSI-4009)

**Incident Handling:**
The mitigation of violations of security policies and recommended practices. (SOURCE: NIST SP 800-61)

**Incident Response Plan (IRP):**
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization’s information system(s). (SOURCE: NIST SP 800-34)

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization’s IT system(s). (SOURCE: CNSSI-4009)

**Indicator of Compromise (IOC):**
A forensic artifact or remnant of an intrusion that can be identified on a host or network. (SOURCE: RSA, DIVISION OF EMC)

**Industrial Control System:**
An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. (SOURCE: NIST)

**Information:**
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. (SOURCE: CNSSI-4009)

**Information Asset:**
An information asset is any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Information Assurance (IA):**
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (SOURCE: NIST SP 800-59; CNSSI-4009)
**Information Owner:**
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. See Information Steward.
(SOURCE: FIPS 200; NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; NIST SP 800-18; CNSSI-4009)

**Information Processing Facilities:**
The physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

**Information Resources:**
Information and related resources, such as personnel, equipment, funds, and information technology.
(SOURCE: FIPS 200; FIPS 199; NIST SP 800-53; NIST SP 800-18; NIST SP 800-60; 44 U.S.C., Sec. 3502; CNSSI-4009)

**Information Security:**
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec.3542)

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
- **Integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- **Availability**, which means ensuring timely and reliable access to and use of information.
(SOURCE: NIST SP 800-66; 44 U.S.C., Sec 3541)

**Information Security Architecture:**
An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.
(SOURCE: NIST SP 800-39)

**Information Security Classification:**
A system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability (also classification, information classification, security classification).
Information Security Continuous Monitoring (ISCM):
Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. (SOURCE: NIST SP 800-137)

Information Security Policy:
Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
(SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-18; CNSSI-4009)

Information Security Risk:
The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk. (SOURCE: NIST SP 800-30)

Information System:
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: FIPS 200; FIPS 199; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-18; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (SOURCE: NIST SP 800-53; CNSSI-4009)

Information System Contingency Plan (ISCP):
Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. (SOURCE: NIST SP 800-34)

Information System Owner:
(a.k.a. Program Manager) Individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60)
**Information System Resilience:**
The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. (SOURCE: NIST SP 800-30)

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. (SOURCE: NIST SP 800-39)

**Information System Security Officer (ISSO):**
Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-37; NIST SP 800-53)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-53A; NIST SP 800-60)

**Information System-Related Security Risks:**
Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation). See Risk. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

**Information Systems Security Officer (ISSO):**
Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: CNSSI-4009)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-39)

**Information Technology:**
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

1. Requires the use of such equipment; or
2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C., Sec. 11101 and Sec 1401)
Information Technology Resources:
Information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants)

Information Type:
A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

Infrastructure as a Service:
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
(SOURCE: Cloud Security Alliance)

Ingress Filtering:
Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network. (SOURCE: PCI DSS GLOSSARY)

Injection Flaws:
Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection.
(SOURCE: PCI DSS GLOSSARY)

Insecure Protocol/Service/Port:
A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that transmit data or authentication credentials (for example, password/passphrase) in clear-text over the Internet, or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. (SOURCE: PCI DSS GLOSSARY)

Inside Threat:
An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)
**Integrity:**
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-37; NIST SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (SOURCE: FIPS 140-2)

The property whereby an entity has not been modified in an unauthorized manner.
(SOURCE: CNSSI-4009)

**Integrity Check Value:**
Checksum capable of detecting modification of an information system. (SOURCE: CNSSI-4009)

**Intellectual Property:**
Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. (SOURCE: NIST SP 800-32)

Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.
(SOURCE: CNSSI-4009)

**Interconnection Security Agreement (ISA):**
An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (SOURCE: NIST SP 800-47)
A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection. (SOURCE: CNSSI-4009)

**Interface:**
A shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these. (SOURCE: Wikipedia)
Common boundary between independent systems or modules where interactions take place.
(SOURCE: CNSSI-4009)
**Internal Network:**
A network where:

(a) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or

(b) cryptographic encapsulation or similar security technology provides the same effect.

An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Internal Revenue Service (IRS) Publication (Pub) 1075:**
This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Taxpayer Information (FTI). (SOURCE: IRS PUB. 1075)

**Internal Security Controls:**
Hardware, firmware, or software features within an information system that restrict access to resources only to authorized subjects. (SOURCE: CNSSI-4009)

**Internal Security Testing:**
Security testing conducted from inside the organization’s security perimeter. (SOURCE: NIST SP 800-115)

**International Organization for Standardization (ISO):**
Non-governmental organization consisting of a network of the national standards institutes. (SOURCE: PCI DSS GLOSSARY)

**Internet:**
The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share

a. the protocol suite specified by the Internet Architecture Board (IAB), and

b. the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

(SOURCE: CNSSI-4009)

**Internet Group Management Protocol (IGMP):**
A communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. (SOURCE: Wikipedia)

**Internet of Things (IoT):**
The network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. (SOURCE: Wikipedia)
Internet Message Access Protocol (IMAP):
An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server. (SOURCE: PCI DSS GLOSSARY)

Internet Protocol (IP):
Standard protocol for transmission of data from (SOURCE to destinations in packet-switched communications networks and interconnected systems of such networks. (SOURCE: CNSSI-4009)

Internet Protocol Telephony (IP Telephony):
See Voice over Internet Protocol (VoIP).

Interoperability:
The ability of making systems and organizations to work together (inter-operate). While the term was initially defined for information technology or systems engineering services to allow for information exchange, a more broad definition takes into account social, political, and organizational factors that impact system to system performance. (SOURCE: Wikipedia)

Intranet:
A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). (SOURCE: CNSSI-4009)

Intrusion:
Unauthorized act of bypassing the security mechanisms of a system. (SOURCE: CNSSI-4009)

Intrusion Detection Systems (IDS):
Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
(SOURCE: CNSSI-4009)

Intrusion Prevention Systems (IPS):
Network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. (SOURCE: Wikipedia)

IP Security (IPsec):
Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment. (SOURCE: CNSSI-4009)

ISO27000:
A family of standards published by the International Organization for Standardization designed to keep information assets secure. ISO 27001 provides requirements for an information security management system. (SOURCE: ISO WEBSITE)
**IT Governance:**
The leadership, organizational structures, and processes that ensure that the enterprise’s IT sustains and extends the enterprise’s strategies and objectives. (SOURCE: The IT Governance Institute)

**IT Infrastructure Library (ITIL):**
A public framework that describes best practice in IT service management. (SOURCE: ITIL V3)

A series of publications providing Best Practice guidance for IT Service Management. (SOURCE: Data Governance Institute)

**IT Portfolio Management:**
A key function of IT Governance, IT portfolio management is the formal process for managing IT assets such as software, hardware, middleware, an IT project, internal staff, an application or external consulting. (SOURCE: Data Governance Institute)

**IT Security Architecture:**
A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. (SOURCE: NIST SP 800-27)

**IT Security Awareness:**
The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. (SOURCE: NIST SP 800-50)

**IT Security Awareness and Training Program:**
Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed. (SOURCE: NIST SP 800-50; CNSSI-4009)

**IT Security Policy:**
The “documentation of IT security decisions” in an organization.

NIST SP 800-12 categorizes IT Security Policy into three basic types:
1. **Program Policy**—high-level policy used to create an organization’s IT security program, define its scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.
2. **Issue-Specific Policies**—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.
3. **System-Specific Policies**—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization’s electronic mail (email) policy or fax security policy. (SOURCE: NIST SP 800-35)
IT Security Training:
IT Security Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues.

The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. (SOURCE: NIST SP 800-50)

IT Service Management (ITSM):
The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process and Information Technology. (Baseline IT definition) (SOURCE: Data Governance Institute)

IT-Related Risk:
The net mission/business impact considering
1. The likelihood that a particular threat (SOURCE will exploit, or trigger, a particular information system vulnerability, and
2. The resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:
   • Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information;
   • Non-malicious errors and omissions;
   • IT disruptions due to natural or man-made disasters; or
   • Failure to exercise due care and diligence in the implementation and operation of IT.
(SOURCE: NIST SP 800-27)

Jailbreaking:
Modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

JAVA:
A computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to bytecode (class file) that can run on any Java virtual machine (JVM) regardless of computer architecture.
(SOURCE: Wikipedia)

JavaScript (JS):
A dynamic computer programming language most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. (SOURCE: Wikipedia)
Kerberos:
A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users. (SOURCE: NIST SP 800-63)

A means of verifying the identities of principals on an open network. It accomplishes this without relying on the authentication, trustworthiness, or physical security of hosts while assuming all packets can be read, modified and inserted at will. It uses a trust broker model and symmetric cryptography to provide authentication and authorization of users and systems on the network. (SOURCE: NIST SP 800-95)

Key:
A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: CNSSI-4009)

A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include:
1. The computation of a digital signature from data, and
2. The verification of a digital signature.
(SOURCE: FIPS 186)

Key Exchange:
The process of exchanging public keys in order to establish secure communications.
(SOURCE: NIST SP 800-32; CNSSI-4009)

Key Logger:
A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures. (SOURCE: NIST SP 800-82)

Key Management:
The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. (SOURCE: FIPS 140-2; CNSSI-4009)

Key Management Infrastructure (KMI):
All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.
(SOURCE: CNSSI-4009)
**Key Pair:**
Two mathematically related keys having the properties that

1. one key can be used to encrypt a message that can only be decrypted using the other key, and
2. even knowing one key, it is computationally infeasible to discover the other key. (SOURCE: NIST SP 800-32)

A public key and its corresponding private key; a key pair is used with a public key algorithm. (SOURCE: NIST SP 800-21; CNSSI-4009)

**Known Error:**
A problem that has a documented root cause and a workaround. (SOURCE: ITIL V3)

**Laptop Computer:**
A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. Unlike a mobile device, a laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities. (SOURCE: Modern Technology As Instructional Devices)

**Layer Three Switch:**
Routers that switch based on Layer 3 information, using ASICs/hardware instead of the CPU/software. Layer three switches differ from layer two switches in that they process data faster using different technology. (SOURCE: Wikipedia)

**Layer Two Switch:**
Network switch utilizing Layer 2 Tunneling Protocol (L2TP), an IETF standard that can be used as an alternative protocol to Multiprotocol Label Switching (MPLS) for encapsulation of multiprotocol Layer 2 communications traffic over IP networks. L2TP provides a pseudo-wire service. (SOURCE: Wikipedia)

**Least Functionality:**
The principle of least functionality states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary.

**Least Privilege:**
The security objective of granting users only those accesses they need to perform their official duties. (SOURCE: NIST SP 800-12)

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (SOURCE: CNSSI-4009)

**Least Trust:**
The principal that a security architecture should be designed in a way that minimizes 1) the number of components that require trust, and 2) the extent to which each component is trusted. (SOURCE: CNSSI-4009)
Level of Protection:
Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are:
1. Basic: information systems and networks requiring implementation of standard minimum security countermeasures.
2. Medium: information systems and networks requiring layering of additional safeguards above the standard minimum security countermeasures.
3. High: information systems and networks requiring the most stringent protection and rigorous security countermeasures.
(SOURCE: CNSSI-4009)

Lightweight Directory Access Protocol (LDAP):
Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected internal resources. (SOURCE: PCI DSS GLOSSARY)

Likelihood of Occurrence:
In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. (SOURCE: CNSSI-4009)

Link Encryption:
Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. (SOURCE: NIST SP 800-12)

Encryption of information between nodes of a communications system. (SOURCE: CNSSI-4009)

List-Oriented:
Information system protection in which each protected object has a list of all subjects authorized to access it. (SOURCE: CNSSI-4009)

Local Access:
Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. (SOURCE: NIST SP 800-53; CNSSI-4009)

Local Area Network (LAN):
A group of computers and/or other devices that share a common communications line, often in a building or group of buildings. (SOURCE: PCI DSS GLOSSARY)

Local Authority:
Organization responsible for generating and signing user certificates in a PKI-enabled environment. (SOURCE: CNSSI-4009)
**Logical Partition (LPAR):**
A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces. (SOURCE: PCI DSS GLOSSARY)

**Low Impact:**
The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.
5. causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
6. results in minor damage to organizational assets;
7. results in minor financial loss; or
8. results in minor harm to individuals.
(SOURCE: CNSSI-4009)

**Low-Impact System:**
An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200; CNSSI-4009)

**Mainframe:**
Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.
(SOURCE: PCI DSS GLOSSARY)

**Major Application:**
A major application or system is defined as any system or application that includes one or more of the following characteristics:
- Includes users in more than one agency;
- Costs more than $200,000 to develop and implement (cost includes hardware, software, and contract personnel);
- Any public facing web application; and/or
- Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

**Malicious Applets:**
Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. (SOURCE: CNSSI-4009)
**Malicious Code:**
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Malicious Logic:**
Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (SOURCE: CNSSI-4009)

**Malware:**
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim. (SOURCE: NIST SP 800-83)

See Malicious Code. See also Malicious Applets and Malicious Logic. (SOURCE: NIST SP 800-53; CNSSI-4009)

A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. (SOURCE: NIST SP 800-61)

**Man-in-the-middle Attack (MitM):**
An attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. (SOURCE: NIST SP 800-63)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (SOURCE: CNSSI-4009)

**Management Controls:**
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; FIPS 200)

Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions. (SOURCE: CNSSI-4009)

**Management Security Controls:**
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security. (SOURCE: CNSSI-4009)
Mandatory Access Control (MAC):
A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. (SOURCE: NIST SP 800-44; CNSSI-4009)

Access controls (which) are driven by the results of a comparison between the user’s trust level or clearance and the sensitivity designation of the information. (SOURCE: FIPS 191)

Masking:
In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc. (SOURCE: PCI DSS GLOSSARY)

Masquerading:
When an unauthorized agent claims the identity of another agent, it is said to be masquerading. (SOURCE: NIST SP 800-19)

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. (SOURCE: CNSSI-4009)

Maximum Tolerable Downtime (MTD):
The amount of time mission/business process can be disrupted without causing significant harm to the organization’s mission. (SOURCE: NIST SP 800-34)

Media:
Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (SOURCE: FIPS 200; NIST SP 800-53; CNSSI-4009)

Media Sanitization:
A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: NIST SP 800-88)

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: CNSSI-4009)

Memorandum of Understanding/Agreement (MOU/A):
A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (SOURCE: NIST SP 800-47; CNSSI-4009)

Memory-Scraping Attacks:
Malware activity that examines and extracts data that resides in memory as it is being processed or which has not been properly flushed or overwritten. (SOURCE: PCI DSS GLOSSARY)
**Message Authentication Code (MAC):**
A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection. (SOURCE: NIST SP 800-63; FIPS 201)

A cryptographic checksum that results from passing data through a message authentication algorithm. (SOURCE: FIPS 198)

**Metadata:**
Data about data. The definition and scope of metadata depends upon context. In the context of Information Management, metadata is generally thought of as providing information (what database stores it? what data type is it? how long is the field? etc.) about a data element. Within the context of Data Governance, the term also includes “business” metadata such as the names and roles of Data Stewards. Metadata repositories are employed to store and report on metadata.
(SOURCE: Data Governance Institute)

**MIME:**
See Multipurpose Internet Mail Extensions.

**Minor Application:**
An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. (SOURCE: NIST SP 800-18)

**Mobile Application Management (MAM):**
Mobile Application Management (MAM) and Mobile Application Store (MAS) management perform application monitoring, reporting, security, and deployment. (SOURCE: GSA.gov)

**Mobile Code:**
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009)

A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. (SOURCE: NIST SP 800-28)
**Mobile Device:**
For the purposes of the Mobile Device Management Policy included in this Manual, a Mobile Device is any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.


Other definitions of a Mobile Device include:
Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory).
Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (SOURCE: NIST SP 800-53)

**Mobile Device Management (MDM):**
Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. (SOURCE: whatis.com)

**Mode of Operation:**
An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm. (SOURCE: NIST SP 800-38C)

Description of the conditions under which an information system operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users.
Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode. (SOURCE: CNSSI-4009)

**Moderate Impact:**
The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.

5. Causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
6. Results in significant damage to organizational assets;
7. Results in significant financial loss; or
8. Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

(SOURCE: CNSSI-4009)

**Multi-Homed Connection:**
A host connected to two or more networks or having two or more network addresses. For example, a computer may be connected to multiple Local Area Networks (LANs).

**Multi-Protocol Label Switching (MPLS):**
A standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multi-protocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS).
(SOURCE: Method and System for Detecting A Connection Fault)

**Multifactor Authentication:**
Authentication using two or more factors to achieve authentication. Factors include:
   a. something you know (e.g. password/PIN);
   b. something you have (e.g., cryptographic identification device, token); or
   c. something you are (e.g., biometric). See Authenticator.
(SOURCE: NIST SP 800-53)

**Multiprotocol Label Switching (MPLS):**
A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL. (SOURCE: Wikipedia)

**Multipurpose Internet Mail Extensions (MIME):**
An Internet standard that extends the format of email to support:
   - Text in character sets other than ASCII
   - Non-text attachments
   - Message bodies with multiple parts
   - Header information in non-ASCII character sets
Although MIME was designed mainly for SMTP protocol, its use today has grown beyond describing the content of email and now often includes descriptions of content type in general, including for the web (see Internet media type) and as a storage for rich content in some commercial products. Virtually all human-written Internet email and a large proportion of automated email are transmitted via SMTP in MIME format. Internet email is so closely associated with the SMTP and MIME standards that it is sometimes called SMTP/MIME email. (SOURCE: Wikipedia)

**Mutual Authentication:**
Occurs when parties at both ends of a communication activity authenticate each other.
(SOURCE: NIST SP 800-32)

The process of both entities involved in a transaction verifying each other. (SOURCE: CNSSI-4009)
National Institute of Standards and Technology:
A measurement standards laboratory that is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to: Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

The Information Technology Laboratory (ITL), one of several components within NIST, publishes standards concerning information security. (SOURCE: Wikipedia)

Need-To-Know:
A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms ‘need-to-know” and “least privilege” express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (SOURCE: CNSSI-4009)

Network:
Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (SOURCE: NIST SP 800-53; CNSSI-4009)

Network Access:
Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (SOURCE: NIST SP 800-53; CNSSI-4009)

Network Access Control (NAC):
A feature provided by some firewalls that allows access based on a user’s credentials and the results of health checks performed on the telework client device. (SOURCE: NIST SP 800-41)

Network Address Translation (NAT):
A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema. (SOURCE: NIST SP 800-41)

Network Resilience:
A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. (SOURCE: CNSSI-4009)

Network Security Scan:
Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals. (SOURCE: PCI DSS GLOSSARY)
**Network Sniffing:**
A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique. (SOURCE: NIST SP 800-115)

**Network Time Protocol (NTP):**

**Network Weaving:**
Penetration technique in which different communication networks are linked to access an information system to avoid detection and trace-back. (SOURCE: CNSSI-4009)

**Network-attached Storage (NAS):**
A file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients. (SOURCE: Wikipedia)

**Network-Level Connection:**
The connection provides access to a State Agency’s private network through tunneling or a remote desktop access architecture and the software and data that reside on the internal information assets. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Non-Console Access:**
Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks. (SOURCE: Payment Card Industry Data Security Standards (PCI-DSS))

**Nonpublic Information:**
Information that the employee obtains, or is provided access to, during his/her employment with the State of New Jersey that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:

- (f) Is designated by the State or the Agency for which the Employee works as nonpublic information;
- (g) Contains markings such as “Confidential”, “Internal”, “Restricted”, or similar language, or is considered sensitive information;
- (h) Contains information that must be protected by State or Federal Statute, State or Agency policy, or other regulation;
- (i) Is provided to the State or the Agency for which the employee works by customers or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or

Contains information related to the internal State or Agency capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls. (SOURCE: State of New Jersey Statewide Information Security Manual)
**Non-Repudiation:**
Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. (SOURCE: CNSSI-4009; NIST SP 800-60)

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (SOURCE: NIST SP 800-53; NIST SP 800-18)

It is the security service by which the entities involved in a communication cannot deny having participate. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin), and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery). (SOURCE: FIPS 191)

A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory). (SOURCE: FIPS 186)

**Null:**
Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes. (SOURCE: CNSSI-4009)

**Object:**
A passive entity that contains or receives information. (SOURCE: NIST SP 800-27)

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains. (SOURCE: CNSSI-4009; NIST SP 800-53)

**Off-line Attack:**
An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. (SOURCE: NIST SP 800-63)

**One-Way Hash Algorithm:**
Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature). (SOURCE: NIST SP 800-49; CNSSI-4009)

**Online Attack:**
An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets. (SOURCE: NIST SP 800-63)
Open Shortest Path First (OSPF):

Open Web Application Security Project (OWASP):
A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (SOURCE: PCI DSS GLOSSARY)

Operational Technology:
The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment. (SOURCE: Wikipedia)

Organizational Information Security Continuous Monitoring:
Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data-driven risk management decisions. (SOURCE: NIST SP 800-137)

Outside Threat:
An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)

Overwrite Procedure:
A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns. (SOURCE: CNSSI-4009)

Packet Filter:
A routing device that provides access control functionality for host addresses and communication sessions. (SOURCE: NIST SP 800-41)

Packet Sniffer:
Software that observes and records network traffic. (SOURCE: CNSSI-4009)

Parity:
Bit(s) used to determine whether a block of data has been altered. (SOURCE: CNSSI-4009)

Partitioning:
A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file. (SOURCE: ISACA)
Passive Attack:
An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).
(SOURCE: NIST SP 800-63)

An attack that does not alter systems or data. (SOURCE: CNSSI-4009)

Passive Security Testing:
Security testing that does not involve any direct interaction with the targets, such as sending packets to a target. (SOURCE: NIST SP 800-115)

Password:
A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. (SOURCE: NIST SP 800-63)

A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. (SOURCE: FIPS 181)

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (SOURCE: FIPS 140-2)

A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. (SOURCE: CNSSI-4009)

Password Cracking:
The process of recovering secret passwords stored in a computer system or transmitted over a network. (SOURCE: NIST SP 800-115)

Password Protected:
The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered. (SOURCE: NIST SP 800-72)

The ability to protect the contents of a file or device from being accessed until the correct password is entered. (SOURCE: NIST SP 800-124)

Patch:
An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (SOURCE: NIST SP 800-123)

Patch Management:
The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. (SOURCE: CNSSI-4009)
**Payment Card Industry (PCI):**
The term refers to the Payment Card Industry Security Standards Council, a council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The PCI Council formed a body of security standards known as the PCI Data Security Standards, (PCI DSS), and these standards consist of 12 significant requirements including multiple sub-requirements that contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines. By complying with qualified assessments of these standards, businesses can become accepted by the PCI Standards Council as compliant with the 12 requirements, and thus receive a compliance certification and a listing on the PCI Standards Council website. Compliance efforts and acceptance must be completed on a periodic basis. (SOURCE: Wikipedia)

**Payment Card Industry Data Security Standard (PCI DSS):**
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. (SOURCE: Wikipedia)

**Private Branch Exchange (PBX):**
A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

**Penetration Testing:**
A test methodology in which assessors, using all available documentation (e.g., system design, code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (SOURCE: NIST SP 800-53A; NIST SP 800-53; CNSSI-4009)

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. (SOURCE: NIST SP 800-115)

**Perishable Data:**
Information whose value can decrease substantially during a specified time. A significant decrease in value occurs when the operational circumstances change to the extent that the information is no longer useful. (SOURCE: CNSSI-4009)
**Personal Firewall:**
A utility on a computer that monitors network activity and blocks communications that are unauthorized. (SOURCE: NIST SP 800-69)

**Personal Identification Number (PIN):**
A password consisting only of decimal digits. (SOURCE: NIST SP 800-63)

A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (SOURCE: FIPS 201)

An alphanumeric code or password used to authenticate an identity. (SOURCE: FIPS 140-2)

A short numeric code used to confirm identity. (SOURCE: CNSSI-4009)

**Personal Information (PI):**
An individual's first name or first initial and last name linked with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or State identification card number; or
3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. [N.J.S.A. 2C:56:8-161]

“Personal Information” as defined by N.J.S.A. 39:2-3.3 “Personal Information” means information that identifies an individual, including an individual’s photograph; social security number; driver identification number; name; address other than the five-digit zip code; telephone number; and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status. [N.J.S.A. 39:2-3.3]

**Personally Identifiable Information (PII):**
Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. (SOURCE: CNSSI-4009)

Any information about an individual maintained by an agency, including

a. any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and

b. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(SOURCE: NIST SP 800-122)
**Phishing:**  
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: NIST SP 800-83)

Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: CNSSI-4009)

A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. (SOURCE: NIST SP 800-115)

**PII Confidentiality Impact Level:**  
The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (SOURCE: NIST SP 800-122)

**Plaintext:**  
Data input to the Cipher or output from the Inverse Cipher. (SOURCE: FIPS 197)

Intelligible data that has meaning and can be understood without the application of decryption. (SOURCE: NIST SP 800-21)

Unencrypted information. (SOURCE: CNSSI-4009)

**Platform as a Service:**  
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (SOURCE: Cloud Security Alliance)

**Policy-Based Access Control (PBAC):**  
A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, and heuristics). (SOURCE: CNSSI-4009)

**Port Scanning:**  
Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). (SOURCE: CNSSI-4009)

**Portable Storage Device:**  
An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory). (SOURCE: NIST)
Portability:
Usability of the same software in different IT environments. The pre-requisite for portability is the
generalized abstraction between the application logic and system interfaces. When software with the
same functionality is produced for several computing platforms, portability is the key issue for

Portable Document Format (PDF):
A file format used to present documents in a manner independent of application software, hardware,
and operating systems. (SOURCE: Wikipedia)

Portal:
A high-level remote access architecture that is based on a server that offers teleworkers access to one
or more applications through a single centralized interface. (SOURCE: NIST SP 800-46)

Post Office Protocol v3 (POP3):
Application-layer protocol used by e-mail clients to retrieve e-mail from a remote server over a TCP/IP
connection. (SOURCE: PCI DSS GLOSSARY)

Potential Impact:
The loss of confidentiality, integrity, or availability could be expected to have:
1. A limited adverse effect (FIPS 199 low);
2. A serious adverse effect (FIPS 199 moderate); or
3. A severe or catastrophic adverse effect (FIPS 199 high) on organizational operations,
   organizational assets, or individuals.
(SOURCE: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 199)

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect;
a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations,
organizational assets, or individuals. (SOURCE: FIPS 200; CNSSI-4009)

Precursor:
A sign that an attacker may be preparing to cause an incident. (SOURCE: NIST SP 800-61; CNSSI-4009)

Predisposing Condition:
A condition that exists within an organization, a mission/business process, enterprise architecture, or
information system including its environment of operation, which contributes to (i.e., increases or
decreases) the likelihood that one or more threat events, once initiated, will result in undesirable
consequences or adverse impact to organizational operations and assets, individuals, other
organizations, or the Nation. (SOURCE: NIST SP 800-30)

Print Suppression:
Eliminating the display of characters in order to preserve their secrecy. (SOURCE: CNSSI-4009)
Privacy:
Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy. (SOURCE: NIST SP 800-32)

Freedom from unauthorized intrusion or disclosure of information about an individual (SOURCE: ISACA)

Privacy Impact Assessment (PIA):
An analysis of how information is handled:
1. to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
2. to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
3. to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
(SOURCE: NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI-4009; OMB Memorandum 03-22)

Private Key:
The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. (SOURCE: NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:
1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt keys that were encrypted by the corresponding public key, or
4. Compute a shared secret during a key-agreement transaction.
(SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2)

In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. (SOURCE: CNSSI-4009)

Private Network:
Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers. (SOURCE: PCI DSS GLOSSARY)

Privilege:
A right granted to an individual, a program, or a process. (SOURCE: CNSSI-4009)

Privileged Account:
An information system account with approved authorizations of a privileged user. (SOURCE: CNSSI-4009; NIST SP 800-53)
Privileged User:
A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (SOURCE: NIST SP 800-53; CNSSI-4009)

Probe:
A technique that attempts to access a system to learn something about the system. (SOURCE: CNSSI-4009)

Problem:
A cause of one or more incidents. (SOURCE: ITIL V3)

Process:
A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. (SOURCE: ITIL V3)

Process Manager:
An individual accountable for operational management of a process. There may be several process managers for one process and the process manager role is often assigned to the same person carrying out the process owner role. (SOURCE: ITIL V3)

Programmable Logic Controller (PLC) or Programmable Controller:
An industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis. (SOURCE: Wikipedia)

Promiscuous Mode:
A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations. (SOURCE: NIST SP 800-94)

Protected Health Information:
The term Protected Health Information, is composed from two definitions in Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996): Health Insurance Portability and Accountability Act of 1996: Administrative Simplification. These statutory definitions are of health information and individually identifiable health information.

Health information means any information, whether oral or recorded in any form or medium, that:

(a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and:

(a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   (i) That identifies the individual; or

   (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information means individually identifiable health information [defined above]:

(a) Except as provided in paragraph (b) of this definition, that is:

   (i) Transmitted by electronic media;

   (ii) Maintained in electronic media; or

   (iii) Transmitted or maintained in any other form or medium.

(b) Protected health information excludes individually identifiable health information in:

   (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

   (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

   (iii) Employment records held by a covered entity in its role as employer.

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

With those definitions in place, the question becomes: what elements comprise protected health information such that if they were removed, items (i) and (ii) of (b) in the definition of individually identifiable health information would not obtain. The answer is in the de-identification standard and its two implementation specifications of the HIPAA Privacy Rule [45 CFR 164.514]:

(a) Standard: de-identification of protected health information. Health information [defined above] that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

   (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information; and

   (ii) Documents the methods and results of the analysis that justify such determination; or

2)
(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

a. Names;

b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   
   (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   
   (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

d. Telephone numbers;

e. Fax numbers;

f. Electronic mail addresses;

g. Social security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
(iii) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

a. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

b. Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(SOURCE: HIPAA)

Protocol:
Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (SOURCE: CNSSI-4009)

Proxy:
A proxy is an application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email. (SOURCE: NIST SP 800-44; CNSSI-4009)

Proxy Agent:
A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device. (SOURCE: CNSSI-4009)

Proxy Server:
A server that services the requests of its clients by forwarding those requests to other servers. (SOURCE: CNSSI-4009)

Public Key (Asymmetric) Cryptographic Algorithm:
A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. (SOURCE: FIPS 140-2)
Public Key:
The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. (SOURCE: FIPS 201; NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used, for example, to:
1. Verify a digital signature that is signed by the corresponding private key,
2. Encrypt keys that can be decrypted by the corresponding private key, or
3. Compute a shared secret during a key-agreement transaction. (SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2; CNSSI-4009)

Public Key Certificate:
A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key. (SOURCE: NIST SP 800-63)

A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority). (SOURCE: FIPS 196)

A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. (SOURCE: FIPS 140-2)

Public Key Infrastructure (PKI):
A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. (SOURCE: NIST SP 800-32; NIST SP 800-63)

An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. (SOURCE: FIPS 196)

A Framework that is established to issue, maintain, and revoke public key certificates. (SOURCE: FIPS 186)

A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system. (SOURCE: FIPS 201)

The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (SOURCE: CNSSI-4009)
Quality of Service (QoS):
The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.
(SOURCE: CNSSI-4009)

Rainbow Table Attack:
A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data (SOURCE, usually for cracking password or cardholder data hashes.
(SOURCE: PCI DSS GLOSSARY)

Reciprocity:
Mutual agreement among participating enterprises to accept each other’s security assessments in order to reuse information system resources and/or to accept each other’s assessed security posture in order to share information.
(SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-39)

Record:
According to the State of New Jersey Open Public Records Act, P.L. 2001, CHAPTER 404 N.J.S. 47:1A-1 et seq., a "Government record" or "record" means any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, maintained or kept on file in the course of his or its official business by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by any such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof. The terms shall not include inter-agency or intra-agency advisory, consultative, or deliberative material.

According to N.J.S.A. 47:3-20, a "Record" or "records" means: pursuant to P.L. 1953, c.410, § 2 as amended by P.L. 1994, c.140, § 3 (N.J.S.A 47:3-16), any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound-recording or similar device, or any copy thereof which has been made or is required by law to be received for filing, indexing, or reproducing by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received by any such officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of the information contained therein.
Records:
The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). (SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. [44 U.S.C. SEC. 3301] (SOURCE: FIPS 200)

Records Management:
The process for tagging information for records-keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements. (SOURCE: CNSSI-4009)

Recovery Point Objective (RPO):
The point in time to which data must be recovered after an outage. (SOURCE: NIST SP 800-34)

Recovery Procedures:
Actions necessary to restore data files of an information system and computational capability after a system failure. (SOURCE: CNSSI-4009)

Recovery Time Objective (RTO):
The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes. (SOURCE: SP800-34)

Red Team:
A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. (SOURCE: CNSSI 4009-2015)

Remanence:
Residual information remaining on storage media after clearing. See Magnetic Remanence and Clearing. (SOURCE: CNSSI-4009)

Remediation:
The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. (SOURCE: NIST SP 800-40)

The act of mitigating a vulnerability or a threat. (SOURCE: CNSSI-4009)
Remediation Plan:
A plan to perform the remediation of one or more threats or vulnerabilities facing an organization’s systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation. (SOURCE: NIST SP 800-40)

Remote Access:
Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). (SOURCE: NIST SP 800-53)

Access by users (or information systems) communicating external to an information system security perimeter. (SOURCE: NIST SP 800-18)

The ability for an organization’s users to access its nonpublic computing resources from external locations other than the organization’s facilities. (SOURCE: NIST SP 800-46)

Remote Desktop Access Architecture:
A high-level remote access architecture that gives a user the ability to remotely control a particular computer at their agency from an external network. Remote desktop access architecture includes, but is not limited to, systems (local and remote) and software (e.g. Cisco AnyConnect, Citrix, GoToMyPC, Verisign Identity Protection (VIP)) that is used to facilitate and secure the remote session. The specific technologies utilized in a remote desktop access architecture are determined by the New Jersey Office of Information Technology. (SOURCE: State of New Jersey Statewide Information Security Manual)

Removable Media:
Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices. (SOURCE: CNSSI-4009; NIST SP 800-53)

Replay Attacks:
An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (SOURCE: CNSSI-4009)

Report on Compliance (ROC):
Report documenting detailed results from an entity’s PCI DSS assessment. (SOURCE: PCI DSS GLOSSARY)

Repository:
A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory. (SOURCE: NIST SP 800-32)
Representational State Transfer (REST):
A software architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements. (SOURCE: Wikipedia)

Residual Risk:
The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat. (SOURCE: NIST SP 800-33)

Portion of risk remaining after security measures have been applied.
(SOURCE: CNSSI-4009; NIST SP 800-30)

Residue:
Data left in storage after information-processing operations are complete, but before degaussing or overwriting has taken place. (SOURCE: CNSSI-4009)

Resilience:
The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. (SOURCE: NIST SP 800-34)

The ability to continue to:
(i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and
(ii) recover to an effective operational posture in a time frame consistent with mission needs.
(SOURCE: NIST SP 800-137)

Risk:
The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
(SOURCE: FIPS 200; NIST SP 800-60)

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
1. The adverse impacts that would arise if the circumstance or event occurs; and
2. The likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
(SOURCE: NIST SP 800-37; NIST SP 800-53A NIST SP 800-53; CNSSI-4009)
**Risk Analysis:**
The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (SOURCE: NIST SP 800-27)

Examination of information to identify the risk to an information system. See Risk Assessment. (SOURCE: CNSSI-4009)

**Risk Assessment:**
The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). (SOURCE: CNSSI-4009)
**Risk Management:**
The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

1. The conduct of a risk assessment;
2. The implementation of a risk mitigation strategy; and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

(Source: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009; NIST SP 800-82; NIST SP 800-34)

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:

1. The conduct of a risk assessment;
2. The implementation of a risk mitigation strategy; and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

(Source: FIPS 200)

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

(Source: NIST SP 800-39)

**Risk Mitigation:**
Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

(Source: CNSSI-4009; NIST SP 800-30; NIST SP 800-39)

**Risk Monitoring:**
Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions. (Source: NIST SP 800-30; NIST SP 800-39)

**Risk Tolerance:**
The level of risk an entity is willing to assume in order to achieve a potential desired result.

(Source: NIST SP 800-32)

The defined impacts to an enterprise’s information systems that an entity is willing to accept.

(Source: CNSSI-4009)

**Rogue Device:**
An unauthorized node on a network. (Source: NIST SP 800-115)
**Role:**
A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. (SOURCE: CNSSI-4009)

**Role-Based Access Control (RBAC):**
A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (SOURCE: NIST SP 800-95)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Root Cause Analysis:**
A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (SOURCE: NIST SP 800-30; NIST SP 800-39)

**Router:**
Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways. (SOURCE: PCI DSS GLOSSARY)

**Rule-Based Security Policy:**
A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. (SOURCE: NIST SP 800-33; CNSSI-4009)

**S/MIME (NIST)**
A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer’s certificate(s). (SOURCE: NIST SP 800-49)

**Safeguards:**
Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200; CNSSI-4009)
Safety:
Condition of being protected from harm or other non-desirable outcomes. (SOURCE: Wikipedia)

Sanitization:
Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. (SOURCE: FIPS 200)

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. (SOURCE: NIST SP 800-53; CNSSI-4009)

Scalability:
The ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. (SOURCE: WIKIPEDIA)

Scanning:
Sending packets or requests to another system to gain information to be used in a subsequent attack. (SOURCE: CNSSI-4009)

Scoping:
Process of identifying all system components, people, and processes to be included in an assessment. The first step of an assessment is to accurately determine the scope of the review. (SOURCE: PCI DSS GLOSSARY)

Secret Key:
A cryptographic key that is used with a secret-key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (SOURCE: NIST SP 800-57)

A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (SOURCE: CNSSI-4009)

A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term “secret” in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 201)

A cryptographic key that is uniquely associated with one or more entities. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 198)

A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. (SOURCE: FIPS 140-2)
Secure Coding Guidelines:
Philosophy and approach supporting the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities. Through the analysis of thousands of reported vulnerabilities, security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying the insecure coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce or eliminate vulnerabilities in software before deployment. (SOURCE: Wikipedia)

Secure DNS (SECDNS):
Configuring and operating DNS servers so that the security goals of data integrity and (SOURCE authentication are achieved and maintained. (SOURCE: NIST SP 800-81)

Secure Hash Algorithm (SHA):
A hash algorithm with the property that is computationally infeasible
1. To find a message that corresponds to a given message digest, or
2. To find two different messages that produce the same message digest.
(SOURCE: CNSSI-4009)

Secure Hash Standard:
This Standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message). When a message of any length less than $2^{64}$ bits (for SHA-1, SHA-224 and SHA-256) or less than $2^{128}$ bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

The hash algorithms specified in this Standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm. (SOURCE: FIPS 180-4)

Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. (SOURCE: CNSSI-4009)

Secure Shell (SSH):
Protocol suite providing encryption for network services like remote login or remote file transfer. (SOURCE: PCI DSS GLOSSARY)
Secure Socket Layer (SSL):
A protocol used for protecting private information during transmission via the Internet.

Note: SSL works by using a public key to encrypt data that’s transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:” (SOURCE: CNSSI-4009)

Security:
A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. (SOURCE: CNSSI-4009)

Security Assertion Markup Language (SAML):
An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. (SOURCE: NIST SP 800-63)

A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called “assertions,” enhancing the interoperability between disparate applications. (SOURCE: NIST SP 800-95)

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between online business partners. (SOURCE: CNSSI-4009)

Security Attribute:
A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. (SOURCE: FIPS 188)

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. (SOURCE: NIST SP 800-53; CNSSI-4009)

Security Content Automation (SCAP):
A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements. (SOURCE: CNSSI-4009)
Security Control Assessment:
The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

Security Control Baseline:
The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: NIST SP 800-53; FIPS 200)

One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253. (SOURCE: NIST SP 800-53A)

Security Control Effectiveness:
The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance. (SOURCE: NIST SP 800-137)

Security Controls:
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

Security Controls Baseline:
The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: CNSSI-4009)

Security Domain:
A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

A collection of entities to which applies a single security policy executed by a single authority. (SOURCE: FIPS 188)

A domain that implements a security policy and is administered by a single authority. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

Security Impact Analysis:
The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Security Information and Event Management (SIEM) Tool:
Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. (SOURCE: NIST SP 800-128)
Security Objective:
Confidentiality, integrity, or availability.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199)

Security Plan:
Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See ‘System Security Plan’ or ‘Information Security Program Plan.’
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18)

Security Policy:
The statement of required protection of the information objects. (SOURCE: NIST SP 800-27)

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
(SOURCE: FIPS 188; (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

Security Requirements:
Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
(SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Security Safeguards:
Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. (SOURCE: CNSSI-4009)

Security Test & Evaluation (ST&E):
Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. (SOURCE: CNSSI-4009)

Security Testing:
Process to determine that an information system protects data and maintains functionality as intended. (SOURCE: CNSSI-4009)

Sensitive Data:
Data that is private, personal, or proprietary and must be protected from unauthorized access. (SOURCE: Data Governance Institute)

Sensitive Information:
A term to describe any information which requires protection from unauthorized access or disclosure. (SOURCE: State of New Jersey Statewide Information Security Manual)
**Sensitive Personally Identifiable Information (SPII):**
Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. (SOURCE: US DHS)

**Separation of Duties:**
Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process. (SOURCE: PCI DSS GLOSSARY)

**Service:**
A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. (SOURCE: ITIL V3)

**Service Management:**
A set of specialized organizational capabilities for providing value to customers in the form of services. (SOURCE: ITIL V3)

**Service Organization Control (SOC) - 1 Report:**
These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, are specifically intended to meet the needs of the managements of user entities and the user entities’ auditors, as they evaluate the effect of the controls at the service organization on the user entities’ financial statement assertions. These reports are important components of user entities’ evaluation of their internal controls over financial reporting for purposes of comply with laws and regulations such as the Sarbanes-Oxley Act and the user entities’ auditors as they plan and perform audits of the user entities’ financial statements. There are two types of reports for these engagements:

- Type 1 – report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

- Type 2 – report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

The use of these reports is restricted to the management of the service organization, user entities of the service organization and user auditors. (SOURCE: AICPA Website)
Service Organization Control (SOC) - 2 Report:
These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users’ data and the confidentiality and privacy of the information processed by these systems. Examples of stakeholders who may need these reports are, management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls. Use of these reports generally is restricted to parties that have this understanding. The AICPA Guide: Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (currently under development) provides guidance for performing these engagements. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Similar to a SOC 1 report there are two types of report: A type 2, report on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls; and a type 1, report on management’s description of a service organization’s system and the suitability of the design of controls. Use of these reports is generally restricted.

(SOURCE: AICPA Website)

Service Organization Control (SOC) - 3 Report:
These reports are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems used by a service organization to process users’ information, and the confidentiality, or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report.

These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 reports can be freely distributed or posted on a website as a SysTrust for Service Organizations seal. For more information about the SysTrust for Service Organization seal program go to www.webtrust.org.

(SOURCE: AICPA Website)

Service Oriented Architecture (SOA):
An architectural style and discipline that improves IT’s ability to meet business demands. Service-oriented design principles advocate factoring system capabilities into loosely coupled, autonomous components (i.e., services) and making the capabilities available to other system components or external consumers. SOA is not dependent on any particular technology.

(SOURCE: The Burton Group (Gartner))
**Service-Level Agreement (SLA):**
Defines the specific responsibilities of the service provider and sets the customer expectations. (SOURCE: CNSSI-4009)

**Session:**
A semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user (see Login session). A session is set up or established at a certain point in time, and then torn down at some later point. An established communication session may involve more than one message in each direction. A session is typically, but not always, stateful, meaning that at least one of the communicating parts needs to save information about the session history in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. (SOURCE: Wikipedia)

**Session Initiation Protocol (SIP):**
A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. The protocol defines the messages that are sent between endpoints that govern establishment, termination and other essential elements of a call. SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams. SIP can be used for two-party (unicast) or multiparty (multicast) sessions. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games. (SOURCE: Wikipedia)

**Signature:**
A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system. (SOURCE: NIST SP 800-61; CNSSI-4009)

**Signature Certificate:**
A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. (SOURCE: NIST SP 800-32; CNSSI-4009)

**Signed Data:**
Data on which a digital signature is generated. (SOURCE: FIPS 196)

**Simple Mail Transfer Protocol (SMTP):**
An Internet standard for electronic mail (e-mail) transmission. (SOURCE: Wikipedia)

**Simple Network Management Protocol (SNMP):**
An Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. It is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. (SOURCE: Wikipedia)
**Simple Object Access Protocol (SOAP):**
A protocol specification for exchanging structured information in the implementation of web services in computer networks. It relies on XML Information Set for its message format, and usually relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. (SOURCE: Wikipedia)

**Single Point of Failure:**
A resource whose loss will result in the loss of service or production. (SOURCE: ISACA)

**SLA:**
Service Level Agreements - Defines the specific responsibilities of the service provider and sets the customer expectations. (SOURCE: NIST)

**Smartphone:**
A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications. (SOURCE: Wikipedia)

**Social Engineering:**
An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (SOURCE: NIST SP 800-61; CNSSI-4009)

A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. (SOURCE: NIST SP 800-114)

The process of attempting to trick someone into revealing information (e.g., a password). (SOURCE: NIST SP 800-115)

**Social Media:**
The interaction among people in which they create, share or exchange information and ideas in virtual communities and networks. (SOURCE: Wikipedia)

**Social Networking:**
Use of a platform/service to support collaboration among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his social links, and a variety of additional services. Social networking is web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/video/sharing and blogging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network. (SOURCE: Wikipedia)
Software:
Computer programs and associated data that may be dynamically written or modified during execution. (SOURCE: NIST)

Software as a Service (SaaS):
The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (SOURCE: Cloud Security Alliance)

Software Development Life Cycle (SDLC):
Acronym for “system development life cycle” or “software development lifecycle.” Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation. (SOURCE: PCI DSS GLOSARY)

Spam:
The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: NIST SP 800-53)

Unsolicited bulk commercial email messages. (SOURCE: NIST SP 800-45)

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: CNSSI-4009)

Special Character:
Any non-alphanumeric character that can be rendered on a standard American-English keyboard. Use of a specific special character may be application-dependent. The list of special characters follows:
```
` ~ ! @ # $ % ^ & * ( ) _ + | } { " : ? > < [ ] ; ' , . / - =
```
(SOURCE: CNSSI-4009)

Specification:
An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. (SOURCE: NIST SP 800-53A)

Spillage:
Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. (SOURCE: CNSSI-4009)

Split Tunneling:
A computer networking concept that allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application. (SOURCE: Wikipedia)
Spoofing:
“IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source. (SOURCE: NIST SP 800-48)

Spyware:
Software that covertly gathers user information through the user’s Internet connection without the user’s knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (SOURCE: NIST SP 800-53; CNSSI-4009)

SQL Injection:
Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database. (SOURCE: PCI DSS GLOSSARY)

Stakeholder:
Anyone who has a responsibility for, an expectation from or some other interest in the enterprise. (SOURCE: ISACA GLOSSARY)

State:
Intermediate Cipher result that can be pictured as a rectangular array of bytes. (SOURCE: FIPS 197)

Stateful Inspection:
Also called “dynamic packet filtering.” Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected. (SOURCE: PCI DSS GLOSSARY)

Stateless Protocol:
A communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. Examples of stateless protocols include the Internet Protocol (IP) which is the foundation for the Internet, and the Hypertext Transfer Protocol (HTTP) which is the foundation of data communication for the World Wide Web. (SOURCE: Wikipedia)

Storage Area Network (SAN):
A dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. (SOURCE: Wikipedia)
**Strong Authentication:**
The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity’s identity. (SOURCE: CNSSI-4009)

**Strong Cryptography:**
Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption and hashing. Examples of industry-tested and accepted standards and algorithms include: AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). (SOURCE: PCI Payment Card Standards Council)

**Strong Password:**
A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

**Structured Query Language (SQL):**
Computer language used to create, modify, and retrieve data from relational database management systems. (SOURCE: PCI DSS GLOSSARY)

**Subject Matter Expert (SME):**
A person who is an authority in a particular area or topic. (SOURCE: Wikipedia)

**Subscriber:**
A party who receives a credential or token from a CSP (Credentials Service Provider) and becomes a claimant in an authentication protocol. (SOURCE: CNSSI-4009; NIST SP 800-63)

**Supervisory Control and Data Acquisition (SCADA):**
A control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery. (SOURCE: Wikipedia)

**Supply Chain:**
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Symmetric Key:**
A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. (SOURCE: NIST SP 800-63; CNSSI-4009)

A single cryptographic key that is used with a secret (symmetric) key algorithm. (SOURCE: NIST SP 800-21 [2nd Ed])
**System:**
Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (SOURCE: CNSSI-4009)

A system is defined as a discrete set of information technologies including computer hardware, software, databases, etc., organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: NIST)

**System Administrator:**
A person who manages the technical aspects of a system. (SOURCE: NIST SP 800-40)

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (SOURCE: CNSSI-4009)

**System Assets:**
Any software, hardware, data, administrative, physical, communications, or personnel resource within an information system. (SOURCE: CNSSI-4009)

**System Development Life Cycle (SDLC):**
The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (SOURCE: NIST SP 800-34; CNSSI-4009)

**System Integrity:**
The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. (SOURCE: NIST SP 800-27)

Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (SOURCE: CNSSI-4009)

**System Level Object:**
Anything on a system component that is required for its operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components. (SOURCE: PCI DSS GLOSSARY)
**System Security Plan:**
Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200)

The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (SOURCE: CNSSI-4009)

**System Software:**
The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, associated programs, and data. (SOURCE: FIPS 140-2)

**Tablet:**
An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications and they are larger. (SOURCE: Tech Target)

**Tabletop Exercise:**
Test method that presents a limited simulation of a disruption, emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation. (SOURCE: ISO 22399:2007)

**Tailoring:**
The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

**Tampering:**
An intentional event resulting in modification of a system, its intended behavior, or data. (SOURCE: CNSSI-4009)

**Technical Non-Repudiation:**
The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. (SOURCE: NIST SP 800-32)
Telephone Network Protocol (TELNET):
Typically used to provide user-oriented command line login sessions to devices on a network. User credentials are transmitted in clear text. (SOURCE: PCI DSS GLOSSARY)

Terminal Access Controller Access Control System (TACACS):
Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication. (SOURCE: PCI DSS GLOSSARY)

Test:
A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

Third Party:
Any entity that an agency does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents. Third parties can be both 'upstream' (suppliers and vendors) and 'downstream', (distributors and re-sellers) as well as non-contractual parties. (SOURCE: US Office of the Comptroller of the Currency)

Threat:
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; CNSSI-4009; FIPS 200)

The potential source of an adverse event. (SOURCE: NIST SP 800-61)

Threat Assessment:
Formal description and evaluation of threat to an information system. (SOURCE: NIST SP 800-53; NIST SP 800-18)

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. (SOURCE: CNSSI-4009; NIST SP 800-53A)

Threat Event:
An event or situation that has the potential for causing undesirable consequences or impact. (SOURCE: NIST SP 800-30)

Threat Monitoring:
Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security. (SOURCE: CNSSI-4009)
Threat Source:
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent. (SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Timestamp:
A sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. Typically refers to digital date and time information attached to digital data. (SOURCE: Wikipedia)

Token:
Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant’s identity. (SOURCE: NIST SP 800-63)

Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also Cryptographic Token. (SOURCE: CNSSI-4009)

Total Risk:
The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). (SOURCE: NIST SP 800-16)

Tracking Cookie:
A cookie placed on a user’s computer to track the user’s activity on different Web sites, creating a detailed profile of the user’s behavior. (SOURCE: NIST SP 800-83)

Traffic Analysis:
A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g., from the source and destination numbers, or frequency and length of the messages. (SOURCE: NIST SP 800-24)

The analysis of patterns in communications for the purpose of gaining intelligence about a system or its users. It does not require examination of the content of the communications, which may or may not be decipherable. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring (e.g., a shipment has arrived, someone is entering a facility) without necessarily learning an identifier or associated data. (SOURCE: NIST SP 800-98)

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the (SOURCE(s) and destination(s) of the flow, and the flow’s presence, amount, frequency, and duration of occurrence. (SOURCE: CNSSI-4009)
Transmission Security – (TRANSEC):
Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

Note: TRANSEC is that field of COMSEC that deals with the security of communication transmissions, rather than that of the information being communicated. (SOURCE: CNSSI-4009)

Transport Layer Security (TLS):
An authentication and security protocol widely implemented in browsers and Web servers. (SOURCE: NIST SP 800-63)

Trap Door:
A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data.

In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information. (SOURCE: CNSSI-4009)

Trojan Horse:
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (SOURCE: CNSSI-4009)

Trust Anchor:
A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor’s public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. (SOURCE: NIST SP 800-57 Part 1)

An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process [or person] loading the signed software or key). (SOURCE: CNSSI-4009)

A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). (SOURCE: NIST SP 800-63)

Trusted Agent:
Entity authorized to act as a representative of an agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. (SOURCE: NIST SP 800-32; CNSSI-4009)
**Trusted Computer System:**
A system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information. (SOURCE: CNSSI-4009)

**Trustworthiness:**
The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (SOURCE: NIST SP 800-79; CNSSI-4009; NIST SP 800-39)

Security decisions with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities. (SOURCE: FIPS 201)

**Tunneling:**
Technology enabling one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. (SOURCE: CNSSI-4009)

**Twitter:**
An online social networking and microblogging service that enables users to send and read short 140-character text messages, called "tweets". Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the website interface, SMS, or mobile device app. (SOURCE: Wikipedia)

**Two Factor Authentication:**
An approach that provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. (SOURCE: Wikipedia)

**Unauthorized Access:**
Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. (SOURCE: FIPS 191)

Any access that violates the stated security policy. (SOURCE: CNSSI-4009)

**Unauthorized Disclosure:**
An event involving the exposure of information to entities not authorized access to the information. (SOURCE: NIST SP 800-57 Part 1; CNSSI-4009)

**Uniform Resource Locator (URL):**
A specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI. URLs are commonly used for web pages (http), but can also be used for file transfer (ftp), email (mailto) and many other applications. (SOURCE: Wikipedia)
Untrusted Process:
Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms. (SOURCE: CNSSI-4009)

User:
The term “user” refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to State information assets. (State of New Jersey Statewide Information Security Manual)

Individual or (system) process authorized to access an information system. (SOURCE: FIPS 200)

Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009)

An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. (SOURCE: FIPS 140-2)

User Datagram Protocol (UDP):
One of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. (SOURCE: Wikipedia)

User-ID:
Unique symbol or character string used by an information system to identify a specific user. (SOURCE: CNSSI-4009)

Validation:
The process of demonstrating that the system under consideration meets in all respects the specification of that system. (SOURCE: FIPS 201)

Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements). (SOURCE: CNSSI-4009)

Vendor:
A vendor, or a supplier, is a supply chain management term that means anyone who provides goods or services to a company or individuals. A vendor often manufactures inventoriable items and then sells those items to a customer. (SOURCE: Wikipedia)
Verification:
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity’s requirements have been correctly defined, or an entity’s attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (SOURCE: CNSSI-4009)

Virtual LAN (VLAN):
In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. (SOURCE: Wikipedia)

Virtual Machine (VM):
Software that allows a single host to run one or more guest operating systems. (SOURCE: NIST SP 800-115)

Virtual Private Cloud (VPC):
An on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources. (SOURCE: Cloud Security Alliance)

Virtual Private Network (VPN):
VPNs extend a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. (SOURCE: Wikipedia)

Virtualization:
Refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage. (SOURCE: PCI DSS GLOSSARY)

The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). (SOURCE: NIST)

Virus:
A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. (SOURCE: CNSSI-4009)
**Voice over IP (VoIP):**
A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone service. (SOURCE: Wikipedia)

**Vulnerability:**
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-115; FIPS 200)

A weakness in a system, application, or network that is subject to exploitation or misuse. (SOURCE: NIST SP 800-61)

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (SOURCE: CNSSI-4009)

**Vulnerability Scan:**
An automated process to proactively identify security weaknesses in a network or individual system. (SOURCE: ISACA)

**Warm Site:**
An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption. (SOURCE: NIST SP 800-34)

Backup site that typically contains the data links and preconfigured equipment necessary to rapidly start operations, but does not contain live data. Thus, commencing operations at a warm site will (at a minimum) require the restoration of current data. (SOURCE: CNSSI-400)

**Web-Based Connection:**
The connection provides access to one or more applications through a single centralized interface, through a direct application access or portal architecture, typically a web-browser to a portal server located within the demilitarized zone (DMZ). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Web Bug:**
A tiny image, invisible to a user, placed on Web pages in such a way to enable third parties to track use of Web servers and collect information about the user, including IP address, host name, browser type and version, operating system name and version, and cookies. (SOURCE: NIST SP 800-28)

**WiFi Protected Access (WPA):**
Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA. (SOURCE: PCI DSS GLOSSARY)
**Wired Equivalent Privacy (WEP):**
A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is no longer considered a viable encryption mechanism due to known weaknesses. (SOURCE: NIST SP 800-48)

**Workaround:**
Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available. (SOURCE: ITIL V3)

**Worm:**
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code. (SOURCE: CNSSI-4009)

**Zeroization:**
A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. (SOURCE: FIPS 140-2)

A method of erasing electronically stored data, cryptographic keys, and Credentials Service Providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data. (SOURCE: CNSSI)
APPENDIX C - RECORD OF CHANGES

The State Chief Information Security Officer shall update the Record of Changes table below in order to document all new or substantive changes and updates to the existing policies, standards, processes, and guidelines contained in the Manual. Minor changes and corrections such as typographical, spelling, and grammatical errors, formatting changes, and the addition of new key terms do not necessitate entries in the Record of Changes.

The effective date of any added, changed, updated, or deleted policy shall be the date of entry in the Record of Changes table.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Policy/Standard #</th>
<th>Description</th>
<th>CISO Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/5/18</td>
<td>3/5/18</td>
<td>All</td>
<td>Original publication of the SISM</td>
<td></td>
</tr>
</tbody>
</table>

...