



STATE OF NEW JERSEY TECHNOLOGY CIRCULAR Information Security Policy	POLICY NO: 18-02-NJOIT	
	SUPERSEDES: NEW	EFFECTIVE DATE: 07/25/2018
	VERSION: 1.1	LAST REVIEWED: 12/16/2020

1 POLICY

The New Jersey Office of Information Technology (NJOIT) and Chief Technology Officer (CTO) requires compliance with the information security policies, standards, processes, and guidelines contained in the Executive Branch Statewide Information Security Manual published by the New Jersey Office of Homeland Security and Preparedness. The policies, standards, procedures, and guidelines included in the Manual supersede any previous Executive Branch Statewide information security policies, standards, procedures, and guidelines issued prior to March 5, 2018, the effective date.

The following NJOIT policies are replaced by the manual:

- 100 - Information Security Program
- 110 - Security Framework Policy
- 111 - Information Security Managing Exceptions
- 115 - Information Security Risk Management Policy
- 116 - Security Assessment Policy
- 121 - Confidential and/or Personally Identifiable Information
- 130 - Information Asset Classification Control Policy
- 132 - Portable Computing Use and Temporary Worksite Assignment Policy
- 141 - Security Awareness Program Policy
- 142 - Workforce Security Policy
- 152 - Information Disposal and Media Sanitization Policy
- 161 - Operational Security Policy
- 162 - System Planning and Acceptance Policy
- 164 - Backup and Restore Policy
- 166 - Electronic Mail/Messaging Content Policy and Standards
- 168 - Change Management Policy
- 171 - Minimum System Security and Protection Policy
- 172 - Access Control Management Policy
- 173 - Wireless Network Security Policy
- 174 - Network Security Policy



- 176 - Information Security System Monitoring and User Review Policy
- 177 - Password Management Policy
- 179 - Remote Access Policy
- 180 - Security in Application Development Policy
- 181 - Encryption and Digital Signatures Policy
- 182 - System and Services Acquisition Policy
- 183 - Software License Management and Distribution
- 184 - Information Security Vulnerability Management Policy
- 190 - Information Security Incident Management Policy
- 191 - Information Security Incident Management Response Procedure
- 195 - Contingency Planning Policy
- 201 - State of New Jersey On-line Privacy Policy
- 202 - Asset Audit and Accountability Policy
- 205 - Certification and Accreditation Policy
- 1600 - Acceptable Internet Usage
- 1602 -Media Protection Policy
- 1701 - Identification and Authentication Policy

2 AUTHORITY

The Policy is established under the authority of New Jersey Statute NJSA, Sections [C.52:18A-224 through C.52:18A-234](#), known as *"The Office of Information Technology Reorganization Act."*

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:

- 2.1.1 New Jersey Executive Order No. 5 creating the Office of Homeland Security and
- 2.1.2 Preparedness (OHSP) (Corzine, 3/6/2006);
- 2.1.3 New Jersey Executive Order No. 178 creating the New Jersey Cybersecurity and
- 2.1.4 Communications Integration Cell ("NJCCIC") (Christie, 5/20/2015);
- 2.1.5 Domestic Security Preparedness Act, P.L. 2001, C.246;



3 SCOPE

All Executive Branch departments and State agencies (Agencies) are directed to cooperate fully with the NJOIT and the CTO to implement the provisions of the Policy, and to ensure effective use of information technology within the Executive Branch of State Government.

4 PURPOSE

The Statewide Information Security Manual is a set of policies, standards, procedures, and guidelines to assist the Executive Branch of New Jersey State Government 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.

5 COMPLIANCE AND ENFORCEMENT

Non-compliance will be referred to the CTO for appropriate action.

6 ADMINISTRATION

The Policy must be reviewed annually, however the CTO reserves the right to change or amend it at any time.

The Policy shall be administered and monitored by the CTO at 300 Riverview Plaza, Trenton, NJ 08625.

Signature on File

Christopher J. REIN,
Chief Technology Officer

07/25/2018

DATE



DOCUMENT HISTORY

Version	Published Date	CTO	Sections Modified	Description of Modifications
1.0	07/25/2018	Christopher J. REIN	0.0.0	Original Published Date