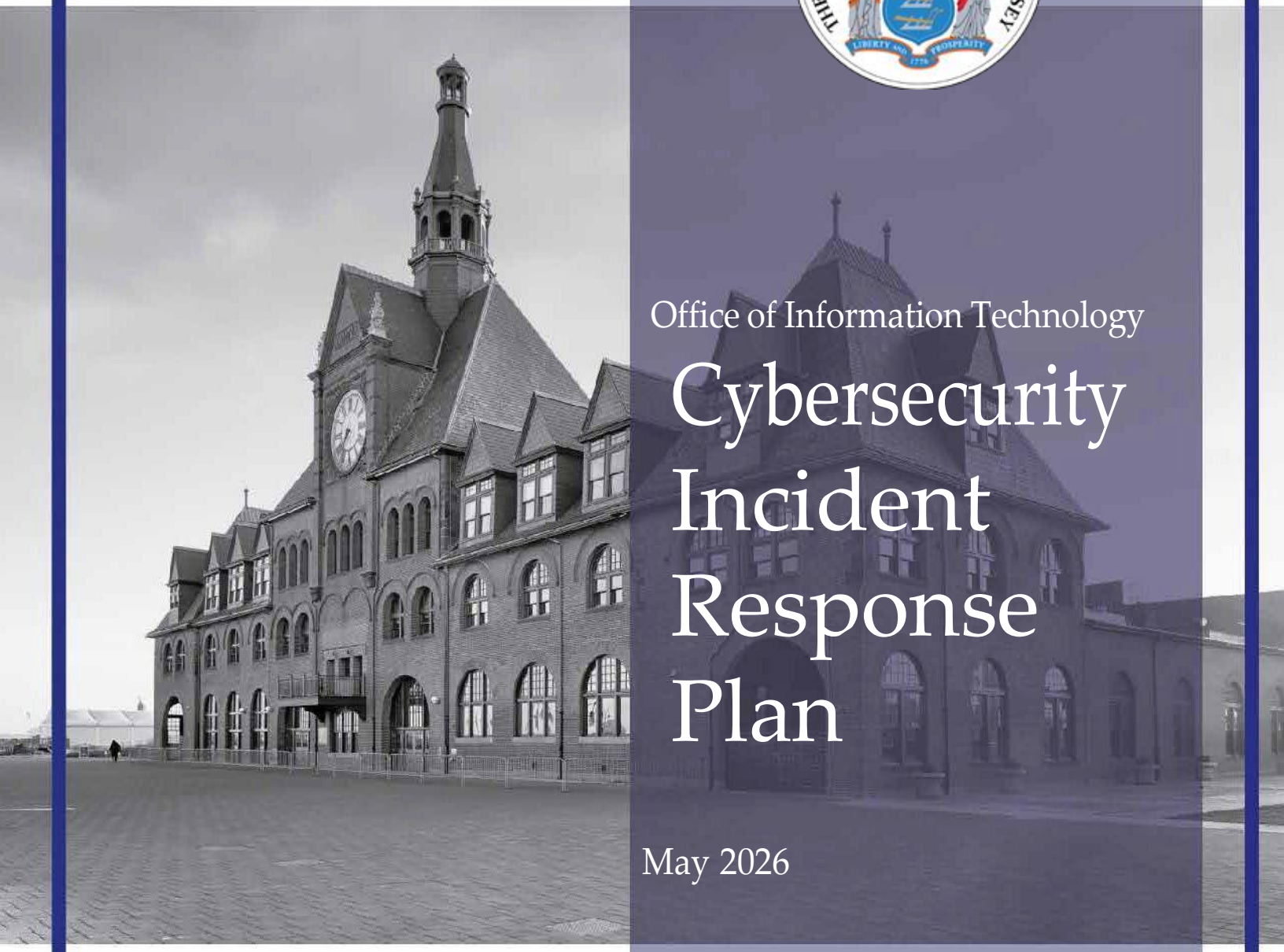

Office of Information Technology

Cybersecurity Incident Response Plan

May 2026

Last Reviewed: May 19th 2026

Table of Contents

1 INTRODUCTION

The New Jersey Office of Information Technology (NJOIT) Cybersecurity Incident Response Plan, hereafter referred to as the "Plan", has been developed in concert with the State of New Jersey (SONJ) Cybersecurity Incident Response Plan for a standard approach for handling Cybersecurity incidents that may compromise the confidentiality, integrity and availability of its information assets. This Plan strives to provide a practical strategy for responding to and managing incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. Each of the following sections is designed to provide agencies with directions on how to manage an incident.

The Cybersecurity Incident Response Plan has been derived from the National Institute of Science and Technology (NIST) Computer Security Incident Handling Guide special publication 800-61 Revision 3 and other industry standard best practices for incident response.

2 SCOPE

The Plan applies to applies to all cybersecurity incidents that affect the confidentiality, integrity and availability of OIT, including agency networks, systems, applications, databases, data, and other information assets owned or controlled by OIT, the agencies or maintained on their behalf. This Plan also applies to any person or device that has authorized access to agency information assets. The Plan does not apply to events that may affect the availability of the agency information assets due to natural disasters, power failures, fires, or other events, that are not considered cybersecurity incidents.

3 RESPONSIBILITY

The OIT Chief Information Security Officer (OIT CISO) is responsible for the development and maintenance of the OIT Plan and has responsibility for the execution of the OIT Plan in collaboration with OIT leadership, the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and Agency Department Heads. The Plan is to be considered a living document that is to be updated to account for changes in agency operations, new threats and risks, lessons learned from previous incidents, new technologies and other relevant factors. On at least an annual basis, the OIT CISO is to review and update the Plan as necessary.

4 DEFINITIONS AND KEY TERMS

User - refers to all OIT full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities

Information Asset - All computer and communications equipment (to include state issued cell phones, tablets, desktops, other communication devices), software, services, data, information, and media, owned or controlled by OIT, agencies or maintained on their behalf.

Event – an event is any observable occurrence in a system or network. Events include a user authenticating to an information system, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt, etc. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Incident - a cybersecurity incident is any adverse event or condition that has the potential to impact the confidentiality, integrity, and availability of agency information assets. Incidents are considered violations of the Enterprise Information Security Policies and Standards or a compromise of agency cybersecurity controls.

Incidents may result from intentional or unintentional actions and may include loss or theft of agency information assets, unauthorized access to agency information assets, introduction of malicious code, or the failure of system security functions to perform as expected.

Data Breach - A data breach is a compromise of the confidentiality of, or the loss of, agency computerized data that results in, or there is a reasonable basis to conclude has resulted in:

- The unauthorized acquisition of Personally Identifiable Information; or
- Access to Personally Identifiable Information that is for an unauthorized purpose, or in excess of authorization.

Personal Information- The term "sensitive personally identifiable information" means any information or compilation of information, in electronic or digital form that includes:

1. An individual's first and last name or first initial and last name in combination with any two of the following data elements:
    - Home address or telephone number;
    - Mother's maiden name;
    - Month, day, and year of birth;
2. A non-truncated social security number, driver's license number, passport number, or alien registration number, or other government-issued unique identification number;
3. Unique biometric data such as a fingerprint, voiceprint, a retina or iris image, or any other unique physical representation;
4. A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, username, or routing code;
5. A username or electronic mail address, in combination with a password or security question and answer that would permit access to an online account; or
6. Any combination of the following data elements:
    - An individual's first and last name or first initial and last name;
    - A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, username, or routing code; or
    - Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

5 INCIDENT RESPONSE METHODOLOGY

The State of New Jersey's approach to handling Cybersecurity incidents, regardless of the incident type, is guided by an incident response methodology that includes a Cybersecurity Incident Lifecycle ("Lifecycle") and a Cybersecurity Incident Framework. The Lifecycle characterizes the continuous efforts agencies make to handle incidents, while at the same time ensuring continuous improvements in the overall security posture of the Executive Branch of State Government or an agency thereof. The Lifecycle also provides agencies with guidance on the various activities that must be carried out to ensure incidents are handled in an effective and efficient manner. The Cybersecurity Incident Response Framework consists of a collection of practices and tools that provide agencies with the ability to categorize, prioritize, communicate, track and document incident response activities. By employing a consistent methodology, the agencies can ensure that their approach to handling incidents is organized and consistent.

5.1 CYBERSECURITY INCIDENT LIFECYCLE

The Cybersecurity Incident Lifecycle consists of four phases: Preparation; Detection & Analysis; Containment, Eradication & Recovery; and Post Incident Activity. Communication and Documentation are parallel activities that are required during each of the Lifecycle's phases.

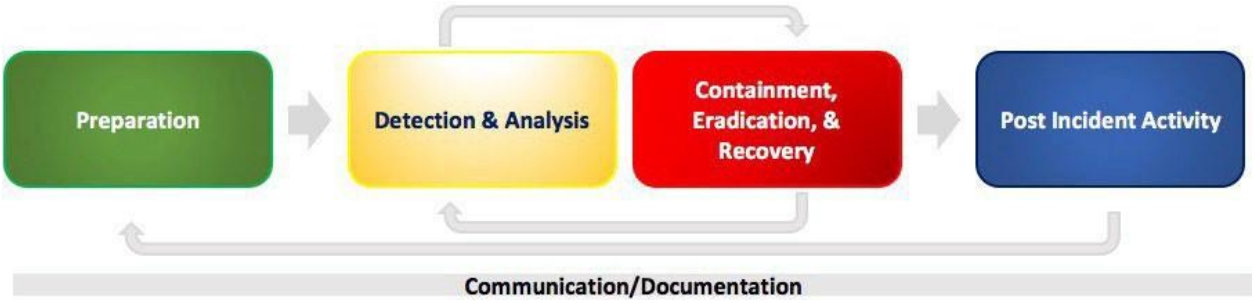

Figure 1 – Information Security Incident Response Life Cycle

5.1.1 Preparation

Preparation includes those activities that enable agencies to respond to an incident. The development and implementation of policies and procedures, the development and implementation of security technologies and tools, training, effective governance and communication plans are all aspects of the preparation phase. Preparation also includes the incorporation of the lessons learned from previous incidents as they form the basis for continuous improvement of agencies' response capabilities.

5.1.2 Detection & Analysis

The Detection & Analysis phase includes the identification and investigation of an incident. Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include intrusion detection and prevention systems, antivirus software, file integrity monitoring software, and security information and event management (SIEM) tools. Incidents may also be detected through manual means, such as problems reported by users, a managed security service provider (MSSP) or
other third parties. During the detection and analysis phase the incident receives an initial categorization and prioritization. An investigation into the incident with corresponding activities including evidence collection, documentation of the incident response activities, etc., are initiated during this phase.

5.1.3 Containment, Eradication & Recovery

	Name	Description
Cat 0	Security Testing	This category is used during agency approved vulnerability and penetration testing activities and other security exercises intended to test the network defenses or responses.
Cat 1	Unauthorized Access	An individual gains logical or physical access without authorization to an agency network, system, application, internal or restricted data, or other information asset.
Cat 2	Denial of Service (DoS)	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.

	Name	Description
Cat 3	Malicious Code	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.
Cat 4	Improper Usage	A user violates the Acceptable Use Policy or other agency Information Security Policies.
Cat 5	Scans, Probes, Attempted Access	Any activity that seeks to access or identify an agency computer, open ports, protocols, services, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Cat 6	Investigation	Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.
Cat 7	Data Breach	A Data Breach is considered a special type of an unauthorized access as it may not only cause serious harm to the agency but also to the individuals to whom the information refers. A data breach is considered: • the compromise of the security, confidentiality, or integrity of sensitive personally identifiable information; • the loss of data that results in, or there is a reasonable basis to conclude, has resulted in, the unauthorized acquisition of sensitive personally identifiable information; • access to Personal Information that is for an unauthorized purpose; or • access to Personal Information that is in excess of authorization. Guidelines for handling a Data Breach involving Personal Information stored or maintained by State agencies is included in Section 9 – Handling Cybersecurity Incidents.

The recovery phase includes all activities involved in the containment of the incident, the eradication of its cause, the restoration of the impacted information assets and the return to normal operations. This phase entails a series of decisions and actions aimed at limiting the damage and preventing further damage from occurring. Agencies should consider factors such as system backups, the risk of continuing operations, and changing passwords, or access controls lists on the compromised systems and data. This phase also involves determining the root cause of the incident, improving system defenses, determining system vulnerabilities and removing the cause of the incident to eliminate possibility of recurrence.

5.1.4 Post Incident Activity

The Post Incident Activity phase involves developing the incident report and disseminating it to appropriate stakeholders; identifying lessons learned from the incident handling process, including the successful and unsuccessful actions taken by an agency in response to the incident; and developing recommendations to prevent future incidents and to improve enterprise security implementation.

5.2 CYBERSECURITY INCIDENT RESPONSE FRAMEWORK

The Cybersecurity Incident Response Framework is intended to provide agency incident responders with a means to categorize the various incident types, determine the severity of an incident, and provide guidance on how to handle the incidents. In addition, the Framework includes guidance on response times, communications, and documentation based on the type and severity of an incident.

5.2.1 Incident Classification

Agencies are to classify incidents according to the following categories: Cat 0 – Security Testing, Cat 1 – Unauthorized Access, Cat 2 – Denial of Service, Cat 3 – Malicious Code, Cat 4 – Improper Usage, Cat 5 – Scans, Probes, Attempted Access, Cat 6 – Investigation, Cat 7 – Data Breach. Incidents that may include activity spanning across multiple categories will be classified according the category associated with the highest severity level. For example, if a reconnaissance scan or probe (Cat 5) leads to the identification of a vulnerability and the subsequent unauthorized access to State systems (Cat 1), the incident will be classified as a Cat 1 incident. The classification of incidents allows for a standardized approach in responding to incidents within each category. In addition, the classification provides a means to track incidents and the effectiveness of agency controls and this Plan. The approach to handling each of these incident types is included in Section 9 – Handling Cybersecurity Incidents.

The following table provides a listing and description of each of the incident category types.

5.2.2 Incident Severity and Prioritization

In addition to the classification of incidents (Cat 1 – Cat 7), there are also three levels of incident severity:

- High
- Medium
- Low

The severity of an 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, and availability of agency systems or information. Agencies may revise an incident's severity level throughout the various incident response phases as dictated by information that is developed.

The following factors must be considered in 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 and/or State - loss of revenue, financial penalties, etc.;
- Sensitivity of the information - Personal Information or other confidential data;
- Probability of propagation - the likelihood that the malware or negative impact will spread or propagate to other systems or agencies;
- Reputational impact to the agency and/or State; 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. The following table provides guidance on differentiating between High, Medium and Low severity ratings along with response times and communications requirements.

Severity	Characteristics (one or more condition present determines the severity)	Response Time	Notifications
High	• Significant adverse impact on a large number systems and/or people • Potential large financial risk or legal liability to the agency and/or State • Threatens the loss of confidentiality of a large number of records containing Sensitive PII or other highly confidential information • Adversely impacts a critical agency system or service • Significant and immediate threat to human safety • High probability of propagating to a large number of other systems and causing significant disruption	Immediately upon discovery of an incident.	• Network Command Center • OIT Cybersecurity Incident Response Team (CSIRT) • OIT CISO, COO, COS • Agency CIO & ISO • Agency Head • NJCCIC • NJSP Cyber Crimes Unit • State Chief Information Security Officer (CISO) • State CTO • OHSP Director • Agency PIO • Attorney General's Office • Governor's Office • Others as dictated by the facts of the incident
Medium	• Adversely impacts a moderate number of agency systems and/or people • Adversely impacts a non-critical enterprise system or service • Moderate risk of propagating and causing further disruption	Within 1 hour of the discovery of an incident.	• OIT Cybersecurity Incident Response Team (CSIRT) • OIT CISO, COO, COS • Agency CIO & ISO • State CTO • Agency Head • NJCCIC • NJSP Cyber Crimes Unit • Others as dictated by the facts of the incident
Low	• Adversely impacts a very small number of non-critical individual systems, services, or people • Disrupts a very small number of network devices or segments • Little risk of propagation and further disruption	Within 1 business day of the discovery of an incident.	• Agency Cybersecurity Incident Response Team (CSIRT) • OIT CISO, COO, COS • State CTO • NJCCIC • Others as dictated by the facts of the incident

5.2.3 Incident Status and Disposition

From the time an incident is discovered through its resolution, agencies should assign both an incident status and disposition status which describes its current stage of the incident response process. The following table describes each status code associated with incidents.

Incident Status	Disposition	Description
New	Pending	An incident has been reported but is pending confirmation and assignment.
Confirmed	Active	An incident has been confirmed by the CSIRT. The incident type and severity have been determined and the response is underway.
Confirmed	Deferred	An incident has been confirmed by the CSIRT. The incident type and severity have been determined but the response is deferred due to resource constraints or other reasons. Deferred responses to high severity incidents are prohibited.
Unfounded	Closed	Insufficient information to confirm an incident, a false positive.
Confirmed	Closed	An incident has been confirmed and the response is complete.

6 ROLES AND RESPONSIBILITIES

6.1 Users

All personnel including full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities (collectively defined as "users") who are provided authorized access to agency information assets are responsible for protecting against their accidental or unauthorized disclosure, modification, or destruction, and for assuring the confidentiality, availability and integrity of State information assets.

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

- Immediate supervisor
- OIT Enterprise Service Desk (1-609-777-1212 or 1-800-622-4357) OIT-ESD@tech.nj.gov
- OIT CISO
- OIT COS/HR Manager
- NJCCIC Incident Reporting Hotline 1-833-465-2242 or OHSP CT Watch: 1-866-472-3365 or https://www.cyber.nj.gov/cyber-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.

Users may also be required to participate in the incident response process by providing information relevant to the incident or by following instructions that can help contain or mitigate the incident.

6.2 OIT Enterprise Service Desk

The agency OIT Enterprise Service Desk acts as a central point of contact for all agency IT issues, including those that may include Executive Branch Agencies. Upon receipt of a call or ticket that may represent an incident the agency IT representative will document the information provided and notify a member of the agency IT team or the agency ISO for analysis and confirmation.

6.3 OIT Cybersecurity Incident Response Team

While any individual may be expected to assist in the response to an incident, an agency Cybersecurity Incident Response Team (CIRT) should be established to promptly and correctly handle incidents that may impact the agency, including its systems, networks, services, data, customers, and employees. The CIRT should be comprised of members from the agency IT team, the ISO, the legal representative, the public information office, the human resources department, and auxiliary agencies or resources, if necessary. Agency Heads should designate an individual with responsibility to act as the CIRT coordinator. This is typically the agency CIO or ISO.

Figure 2 - Agency Incident Response Team

The CSIRT is responsible for carrying out the agency's response to incidents. The CIRT is authorized to take the appropriate steps deemed necessary to contain, mitigate, and resolve an incident in an effective and efficient manner. The CIRT will be supported in its response efforts by the NJCCIC, New Jersey State Police Cyber Crimes Unit, and others, as appropriate. All criminal investigations will be led by the NJSP Cyber Crimes Unit.

The incident's classification, severity, and other factors will dictate which CSIRT members are required to respond to an incident. From the time an incident is reported the CSIRT members who have received the report are responsible for:

- Validating the initial report and declaring an incident as appropriate;
- Determining the type, severity and priority of the incident; and
- Notifying the OIT-CTO, COO, COS, and CISO, and the NJCCIC of the incident

The OIT CTO and OIT CISO, or an authorized designee will act as the Incident Coordinator and determine which CSIRT members play an active role in the investigation and:

- Coordinate the agency's response efforts;
- Engage auxiliary agencies as necessary;
- Escalate incidents to executive management as appropriate;
- Monitor progress of the investigation;
- Ensure evidence gathering, chain of custody, and preservation is appropriate; and
- Prepare a written summary of the incident and corrective action taken

Note: For major incidents a member of the NJCCIC or another qualified individual may be designated as the incident coordinator. In instances where the cybersecurity event is declared by the State CISO as a significant cyber security incident impacting the State of New Jersey, the Cybersecurity Incident Annex of the New Jersey Emergency Operation Plan (EOP) will take effect.

6.4 OIT CSIRT Responsibilities

Entity	CIRT Responsibilities
OIT IT Team	• Design, acquire and implement IT systems and services in a secure manner. • Monitor agency networks, systems, applications, and databases under their purview for indicators of a cybersecurity incident. • Examine logs of agency networks, systems, applications, and databases under their purview for indicators of a cybersecurity incident. • Provides subject matter expertise for technical issues. • Execution of the day-to-day management and security of information systems and services. • Responsible for the selection and management of IT vendors and service providers. • Provides direct support throughout the cybersecurity incident response life cycle. • Provide assistance in the investigation of unauthorized activities and cybersecurity incidents. • As part of the CIRT takes action to respond to cybersecurity incidents. • Take action to contain, eradicate and recover from an incident. • Provide recommendations regarding policy and control enhancements to the Agency ISO.
NJ Office of Homeland Security and Preparedness	• Provide assistance to CIRTs takes action to respond to cybersecurity incidents. • Acts as incident coordinator for large scale incidents • Development and implementation of the Cybersecurity Incident Response Plan. • Collection and analysis of computer evidence related to incidents • Storage and security of evidence collected as part of an incident. • Develops and maintains Cybersecurity Incident Metrics.
NJSP Cyber Crimes Unit	• Lead agency for investigation of incidents deemed to be criminal actions • Collection and analysis of computer evidence in support of criminal investigations. • Provide assistance to CIRTs

Entity	CSIRT Responsibilities
Attorney General's Office/ Agency legal counsel	• Provide advice, counsel, direction and investigative support regarding Cybersecurity incidents. • Provide guidance throughout the investigation on issues relating to privacy of individuals' personal information. • Assist in developing appropriate communication to impacted parties. • Provide guidance and direction regarding how to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers, if needed. • Assesses the need to change privacy policies, procedures, and/or practices to ensure currency with legal and regulatory requirements, or as a result of the breach. • Act as the primary point of contact for outside legal services.
OIT Office of Communications & Digital Services	• Act as the primary media contact for all incidents. • Develop appropriate internal and external communications. • Act as the primary point of contact for external communications and public relations firms. • Aid in the development of the incident response communications plans. • Track and monitor media coverage including social media and respond as appropriate.
OIT Office of Chief of Staff/ Human Resources (HR)	• Provide support to the CIRT during an incident. • Assist in the development, distribution, communication and enforcement of the Enterprise Information Security Policies and Standards • Notifies the agency IT Service Desk of updates to employees' security access privileges according to changes in employment status, including promotions, transfers and terminations. • Administer the new employee orientation program which includes notifying all new hires of their requirement to complete the Cybersecurity Awareness Training. • Assist in the investigation and handling of information security policy violations, as appropriate.
Information Security Governance Committee (ISGC)	• Review reports on significant Cybersecurity incidents, cases of non-compliance, and make recommendations as necessary. • Oversee the response to security incidents which could potentially have a material impact on the Company. • Assist the State Chief Information Security Officer (CISO) in the execution and oversight of the Cybersecurity Incident Response Plan. • Responsible for coordinating communications between the ISIRT and the Executive Leadership Team and Board of Directors, as appropriate.

OIT CIRT Response Team Contact Sheet

To ensure that agencies can contact members of its CIRT the CIRT contact sheet should be completed and provided to all pertinent individuals.

External Resources

Depending on the nature and severity of an incident, the CIRT may enlist additional external resources to aid in the response. External resources include, but are not limited to, breach response services, outside

legal counsel, computer forensics firms, public relation firms, IT security services, IT services, Internet Service Providers (ISPs), law enforcement, and others.

Appendix D contains the contact information for both key CSIRT members and external resources.

7 INCIDENT TRACKING, DOCUMENTATION AND REPORTS

The State of New Jersey Cyber Communications & Integration Cell will maintain a centralized incident tracking system that will be used to record the following information about reported security incidents. The incident tracking system should be used to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences. In addition, OIT will record incidents reported to the Enterprise Service Desk Ticketing System to collect and track respective incidents.

Documentation is a parallel process that runs throughout the Incident Management Lifecycle. All incident response activities will be documented to include artifacts and evidence obtained using methods consistent with chain of custody and confidentiality requirements. All phases of incident response process require detailed documentation of actions taken and the conclusions drawn from analysis.
Detailed documentation assists in determining the correct response and in supplying vital data for conducting follow-up investigation and producing a post-incident report. Documents and artifacts associated with incidents shall be protected commensurate with their sensitivity and are to be protected from tampering. Documentation includes any information that is associated with a specific incident, including all data, including system and network logs, forensics images, IDS logs, backup logs, and any other data or documentation that provides information about the incident, all actions the ISIRT initiates, communications logs, and any information produced by software tools, log files, and similar data produced as part of the ISIRT's response activities.

Post-Incident Report

Individual security incidents may require completion of a Closing Memorandum that provides a summary of the incident, its resolution and any recommendations to help mitigate the risk of a reoccurrence. CIRT personnel will complete and submit to the OIT CISO and the NJCCIC a Closing Memorandum for all High severity Incidents within 30 days of the recovery from an incident. The OIT CISO and the State CISO will review any recommendations in the report and determine additional follow-up actions.

8 HANDLING CYBERSECURITY INCIDENTS

In the process of responding to an incident, many questions arise and problems are encountered, any of which may be different for each incident. This section and the subsequent sections provide process guidelines for handling common incidents and addressing issues. The OIT should consult the OHSP Division of Cybersecurity for questions and incident types not covered by these guidelines.

Legal Counsel

Agency legal counsel and/or the Attorney General's office should be consulted early on in any incident that might represent a violation of criminal law or may involve an employment law matter.

Communications Plan

All communications about an incident or incident response shall be handled by the agency Public Information Office in consultation with the agency Legal Counsel and/or the Attorney General's Office. This includes press releases, responses to media inquiries, website or social media postings, as well as all internal communications on agency Intranet sites or other internal communications vehicles.

Appendix A contains sample communications and notification guidance and documentation.

8.1 HANDLING AN UNAUTHORIZED ACCESS INCIDENT

Unauthorized Access occurs when an individual gains logical or physical access to an agency device network, system, application, data, or other information asset without permission. Unauthorized access provides an attacker with a foothold into the agency environment that may lead to an escalating series of malicious activity. Unauthorized Access is considered a Cat 1 incident type.

Malicious Activity	Possible Indicators or Symptoms
Root/Admin Compromise of System	• Network and host intrusion detection alerts • User reports of system unavailability • Existence of unauthorized security-related tools, exploits or other applications • Unusual traffic to and from the victim system • System configuration changes, including process/service modifications or additions, unexpected open ports, system status changes (restarts, shutdowns), changes to log and audit policies and data, network interface card set to promiscuous mode (packet sniffing), new administrative-level user accounts or groups • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Existence of unexplained local user accounts and usage • Significant changes in expected resource usage • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Unusual operating system and application log messages • Attacker contacts the agency or a third party to say that he or she has compromised a system
Unauthorized Data Modification	• Network and host intrusion detection alerts • Increased resource utilization • User reports of data modification • Modifications to critical files • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage
Unauthorized Use of Standard User Account	• Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools

Malicious Activity	Possible Indicators or Symptoms
Unauthorized Data Access	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • System-recorded access attempts to critical files
Physical Intrusion	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or an unauthorized wireless access point to the network)

The facts determined during the CIRT's response to an Unauthorized Access incident will determine the necessary response activities. This checklist is presented as a guide as opposed to a strict sequence of actions to be followed. During all phases of the response, the ISIRT will ensure all actions and findings are documented and will communicate with the appropriate stakeholders.

INITIAL ACTION

Upon a report of an unauthorized access incident, the OIT CISO and/or agency ISO should be notified immediately. Any source of information that may provide additional insight into the incident should be secured. These include, but are not limited to, the following: SIEM console alerts, email notifications, intrusion detection system (IDS) logs, firewall logs, netflow data, system access logs, etc.

Evaluate the information gathered and determine if an incident response process is to be activated.

At the outset of an incident the following information is to be documented. This represents the minimum information:

- Incident date and time, including time zone;
- Person reporting incident;
- System owner information including name, business unit and phone number;
- System Function (e.g., web server, database server, workstation, etc.);
- System IP Address, hostname, and agency asset tag number;
- Operating System, including version, patches, etc.;
- Antivirus software installed, including version, and latest updates;
- Attacker's IP, hostname, port, and protocol; and
- Method used to identify the incident (e.g., IDS/IPS, audit log analysis, system administrator)

Notify the System Administrator(s), Custodian(s) or user(s) of the impacted system(s) and instruct them to not to use, modify or power off the system(s) until directed by appropriate ISIRT personnel.

DETECTION & ANALYSIS

Evaluate the system or files source for criticality and sensitivity of information and assign a Severity rating based on the findings.

If the compromised information asset is determined to be of high or critical value, or poses substantial exposure to the agency, consider disconnecting or blocking the compromised system from the network or Internet.

The following list includes some of the volatile information that should be collected from the victim system(s) prior to powering down:

- System Date, Time, Time zone
- System Information Summary
- Audit Policy
- ARP Cache
- DNS Cache
- NetBIOS Name Table
- Routing Table
- Current Network Connections
- Running Processes
- Running Services or Daemons
- System, Application, and Security Logs
- The System Registry
- Scheduled Jobs
- Program Started at Boot or User Login
- Users Currently Logged In
- Files Open over the Network
- Open TCP/UDP Ports
- IP Configuration
- Hidden Files/Alternate Data Streams
- Protected System Files
- Various Root Kit Detection Profiling
- Full Memory Dump
- Swap/Tmp File Dump
- Hibernation File Dump
- Dump of Suspicious Processes Running in Memory

Examine all volatile information as well as all external and local response logs obtained to determine the level of compromise (user, root or data). Look for altered system files, added programs, root kits, Bot Nets, back-doors, hidden special files and directories.

If identification of the compromised system is determined to be at a system or root level consider blocking the system from external access if not already blocked earlier.

Determine the scope of compromise by examining network records for potential access to other systems within the agency or in other agencies from the compromised system. If more systems are found to have been accessed run the above identification steps for each suspect system.

Create a forensics image of the impacted system(s) and run forensic analysis on the image to determine the details of the type and nature of the compromise.

Ensure all actions are documented and communicated to relevant stakeholders.

CONTAINMENT, ERADICATION & RECOVERY

If it is determined that the attacker is originating from an external host/network and the attack is escalating, disconnect or block the attacker at the perimeter firewall.

If the compromise is spreading to other systems escalate the incident to appropriate CIRT members and consider disconnecting impacted systems to contain the threat.

Ensure that all system processes related to the compromise have been stopped and removed from the system.

Run a full vulnerability scan of the compromised system(s) and submit the scan report to the System Administrator(s)/Information Custodian(s)/IT Manager for remediation.

Ensure that all files modified or added to the system by the attackers have been removed.

If the compromise was determined to be at a system or root level the system should be wiped and the operating system reinstalled and hardened to prevent a reoccurrence.

Review and restore any affected data modified or deleted from backups, if possible. If the data files are contaminated (i.e. macro virus) ensure they are cleaned before restoring.

Review system configurations to ensure the following are current:

- Versions and patches of all system software
- Auditing and monitoring of systems
- System and data access control lists
- User/System accounts

Rerun a vulnerability scan on the system(s) to ensure all known issues have been remediated.

Continue to document and communicate response activities to all relevant stakeholders.

POST INCIDENT ACTIVITIES

Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.

Document the details of the incident and the steps taken to neutralize the incident and determine the root cause.

Perform an analysis of the following areas to determine where performance could have been improved:

- Whether preparation was adequate;
- Whether detection was prompt and response procedures were adequate;
- Whether the incident was sufficiently contained;
- Whether recovery was adequate; and
- Whether personnel and organization communications were adequate throughout the response to the incident.

Submit any recommendations for enhanced computer security processes.

Complete the Closing Memorandum and submit to the agency ISO and the NJCCIC for review. The Closing Memorandum will be distributed by the agency ISO to only those with a need to know.

8.2 HANDLING A MALICIOUS CODE OUTBREAK

Malicious code incidents include viruses, worms, Trojan horses, keystroke loggers, backdoors, ransomware, and root-kits. Malicious code is considered a Cat 3 incident.

The terms virus and worm are used to define the method in which malicious code spreads rather than the behavior of the malicious code itself. Worms are self-propagating (autonomous) malicious code that uses the network as its transport mechanism and infects other computers on the network by exploiting weaknesses in programs. Viruses depend on the end user to run or execute the malicious code to infect the computer.

Trojan horses, root-kits, and backdoors are used to define the nature of concealment. A Trojan horse conceals the harmful effects of the malicious code by disguising its true destructive nature. Root-kits, on the other hand, modify operating system programs to prevent detection. Backdoor malicious code installs programs that allow an intruder access to the computer by bypassing any authentication mechanisms. Backdoor malicious code is sometimes used by Botnets for remote command and control for remote control. Malicious code incidents may escalate into Cat 1, Unauthorized Access incidents. In addition to the indicators and response guidelines listed below, the response activities for Cat 1 incidents may also be applicable.

Malicious Code	Possible Indicators
A virus/malware that spreads through email infects a host	• Antivirus/Anti-malware software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes • Data files are inexplicably encrypted • Ransom notices are displayed on victim system
A worm that spreads through a vulnerable service infects a system	• Antivirus/Anti-malware software alerts of infected files • Port scans and failed connection attempts targeted at other SONJ systems • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host	• Antivirus/Anti-malware software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between an SONJ system and unknown remote systems • Unusual and unexpected open ports • Unknown processes running • High amounts of network traffic generated by the infected system • Programs start slowly, run slowly, or do not run at all • System instability and crashes

Malicious Code	Possible Indicators
Malicious mobile code on a web site is used to infect an agency system with a virus, worm, or Trojan horse	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious code on a web site exploits vulnerabilities on an agency system	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message	• Original source of the message is not an authoritative computer security group • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others • Urges recipient(s) to download, purchase and run antivirus software

The facts determined during the CIRT's response to a Malicious Code incident will determine the necessary response activities. This checklist is presented as a guide as opposed to a strict sequence of actions to be followed. During all phases of the response the CIRT will ensure all actions and findings are documented and will communicate with the appropriate stakeholders.

INITIAL ACTION

Upon a report of a Malicious Code incident, appropriate IT security personnel and the agency ISO should be notified immediately. Any source of information that may provide additional insight into the incident should be secured. These include but are not limited to the following: virus alerts, email notifications, mail gateway logs, web gateway logs, file integrity logs, intrusion detection system (IDS) logs, firewall logs, system logs, and SIEM logs, etc.

Evaluate the information gathered and determine if an incident response process is to be activated.

At the outset of an incident the following information is to be documented. This represents the minimum information:

- Incident date and time, including time zone
- Person reporting incident
- System owner information including name, business unit and phone number
- System Function (e.g., web server, database server, workstation, etc.)
- System IP Address, hostname, and SONJ asset tag number
- Operating System, including version, patches, etc.
- Antivirus/Anti-malware software installed, including version, and latest updates
- Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)

Notify the System Administrator(s), Custodian(s) or user(s) of the infected system(s) and instruct them to not to use, modify or power off the system(s) until directed by appropriate CIRT personnel.

DETECTION & ANALYSIS

If the malicious code is known to be one of the following: worm, email spammer, keystroke logger, ransomware or other malware that presents a high risk to the confidentiality, integrity and availability of other systems, disconnect the infected system from the agency network or Internet.

The following list includes some of the volatile information that should be collected from the victim system(s) prior to powering down.

- System Date, Time, Time zone
- System Information Summary
- Audit Policy
- ARP Cache
- DNS Cache
- NetBIOS Name Table
- Routing Table
- Current Network Connections
- Running Processes
- Running Services or Daemons
- System, Application, and Security Logs
- The System Registry
- Scheduled Jobs
- Program Started at Boot or User Login
- Users Currently Logged In
- Files Open over the Network
- Open TCP/UDP Ports
- IP Configuration
- Hidden Files/Alternate Data Streams
- Protected System Files
- Various Root Kit Detection Profiling
- Full Memory Dump
- Swap/Tmp File Dump
- Hibernation File Dump
- Dump of Suspicious Processes Running in Memory

Determine the state of anti-virus/anti-malware software: application name, last update of virus signatures, version, etc. If identification of infection has not been determined, obtain a forensic image of the system and run a forensic analysis to determine the details of the type and nature of the malicious code.

Ensure all actions are documented and communicated to relevant stakeholders.

CONTAINMENT, ERADICATION & RECOVERY

If it is determined that the originator of the malicious code is an external system/network and the attack is escalating, consider disconnecting or blocking the attacker at the perimeter firewall.

If the infection is propagating and spreading rapidly disconnect the system from the network.

Ensure that all system processes related to the malicious code have been stopped and removed from the system.

Run a full vulnerability scan of the infected system and submit the scan report to the System Administrator for remediation.

Ensure that all files related to the malicious code have been removed from the system.

If it is not certain that all files infected by the malicious code were discovered, a reformatting/reimage of the system should be accomplished.

Restore the affected system(s) and/or network (using original software media to restore software) to the original configuration with any modifications to preclude reoccurrence of the incident.

Review system configurations to ensure the following are current:

- Versions and patches of all system software;
- Auditing and monitoring of systems;
- System and data access control lists; and
- User/System accounts.

Rerun a vulnerability scan on the system to ensure all known issues have been remediated.

Continue to document and communicate response activities to all relevant stakeholders.

POST INCIDENT ACTIVITIES

Update virus signatures on all agency endpoints and gateways to prevent a reoccurrence of the incident.

Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.

Perform an analysis of the following areas to determine where performance could have been improved:

- Whether preparation was adequate;
- Whether detection was prompt and response procedures were adequate;
- Whether the incident was sufficiently contained;
- Whether recovery was adequate; and
- Whether personnel and organization communications were adequate throughout the response to the incident.

Submit any recommendations for enhanced computer security processes.

Complete the Closing Memorandum and submit to the agency ISO and the NJCCIC for review. The Closing Memorandum will be distributed by the agency ISO to only those with a need to know.

8.3 HANDLING AN INAPPROPRIATE USAGE INCIDENT

An inappropriate usage incident occurs when a user performs actions that violate the Enterprise Information Security Policies and Standards, or other relevant policies. Although such incidents are often not security related, handling them is very similar to handling security-related incidents. Inappropriate Usage is considered a Category 4 Incident.

Agencies may have different processes for handling or investigating inappropriate usage incidents.

Examples of incidents a team might handle are users who:

- Download and install unapproved software, hacking tools, etc.;
- Access or download materials in violation of the Acceptable Use policy;
- Send spam promoting a personal business;
- Email harassing messages to coworkers;
- Set up an unauthorized web site on one of the agency's computers;
- Use file or music sharing services to acquire or distribute pirated materials; and/or
- Transfer sensitive materials from the agency to external locations.

Inappropriate Use	Possible Indicators
Unauthorized service usage	• Network intrusion detection and/or other alerts • Unusual traffic to and from a user's system • New process/software installed and running on an agency computer • New files or directories with unusual names (e.g., "warez" server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • user reports • Application log entries (e.g., Web proxies, FTP servers, email servers)
Access to inappropriate materials	• Network intrusion detection alerts • Web Application Gateway alerts • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media
Attack against external party	• Network intrusion detection alerts • Outside party reports • Network, system, and application log entries
Network host and port enumeration scanning	• Network and host intrusion detection alerts • Increased resource utilization

The facts determined during the CIRT's response to an Inappropriate Use incident will determine the necessary response activities. This checklist is presented as a guide as opposed to a strict sequence of actions to be followed. During all phases of the response the CIRT will ensure all actions and findings are documented and will communicate with the appropriate stakeholders.

INITIAL ACTION

Upon a report of an Inappropriate Usage incident, appropriate agency IT personnel and the agency ISO should be notified immediately. Any source of information that may provide additional insight into the incident should be secured. These include, but are not limited to, the following: user reports, virus alerts, email notifications, mail gateway logs, web gateway logs, file integrity logs, intrusion detection system (IDS) logs, firewall logs, system logs, and SIEM logs, etc.

Evaluate the information gathered and determine if an incident response process is to be activated.

At the outset of an incident the following information is to be documented. This represents the minimum information:

- Incident date and time, including time zone;
- Person reporting incident;
- Suspect information including name, business unit and phone number;
- Suspect's System IP Address, hostname, and agency asset tag number;
- Operating System, including version, patches, etc.; and
- Method used to identify the incident (e.g., IDS, proxy log, audit log analysis, user report)

DETECTION & ANALYSIS

Inappropriate usage incidents are most often detected through user reports, such as seeing inappropriate material on a user's screen or receiving an inappropriate email or instant message. There are usually no precursors of inappropriate usage.

The CIRT should be cautious about assisting with reports of inappropriate usage that are not clearly security incidents – violations of the Enterprise Information Security Policies and Standards or other agency or State policies. For example, a manager might report that an associate seems to be wasting significant time, but the manager has no idea what the employee is doing. The manager might ask the CIRT to monitor the associate's Internet usage and analyze files on the associate's hard drive. The CIRT should verify that the request has been approved by appropriate management and human resources personnel via written approval.

CONTAINMENT, ERADICATION & RECOVERY

Inappropriate usage incidents typically require no containment, eradication, or recovery actions, other than possibly deleting objectionable materials or uninstalling unauthorized software. For most inappropriate usage incidents, evidence acquisition is important. Evidence may be needed for prosecuting or disciplining an individual and for limiting liability by demonstrating that the agency did its best to prevent, detect, and halt the activity. Evidence storage is particularly important because internal users have physical access to many facilities. Addressing the threat of having evidence altered or destroyed may require coordination with the agency's physical security staff.

POST INCIDENT ACTIVITIES

Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.

Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.

Perform an analysis of the following areas to determine where performance could have been improved:

- Whether preparation was adequate;
- Whether detection was prompt and response procedures were adequate;
- Whether the incident was sufficiently contained;
- Whether recovery was adequate; and
- Whether personnel and organization communications were adequate throughout the response to the incident.

Submit any recommendations for enhanced computer security processes.

Complete Closing Memo and distribute to relevant stakeholders.

8.4 HANDLING A DENIAL-OF-SERVICE INCIDENT

A Denial of Service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space. Denial of Service is considered a Cat 2 incident. Distributed denial of service (DDOS) attacks are such that thousands of attacking systems may be employed to flood agency systems with network traffic that would make services unavailable to customers, associates and others. DDOS attacks may render an agency unable to carry out critical business functions.

Examples of DoS attacks are:

- Using all available network bandwidth by generating unusually large volumes of traffic;
- Sending malformed TCP/IP packets to a server so that its operating system will crash;
- Sending illegal requests to an application to crash it;
- Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply or conduct a database query);
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions;
- Broadcasting on the same frequencies used by a wireless network to make the network unusable; and/or
- Consuming all available disk space by creating many large files.

The facts discovered during the CSIRT's response to a Denial-of-Service incident will determine the necessary response activities. The following checklist (under "Initial Action" below) is presented as a guide (as opposed to a strict sequence of actions to be followed). During all phases of the response the CSIRT will ensure all actions and findings are documented and will communicate with the appropriate stakeholders.

INITIAL ACTION

Upon a report of a Denial-of-Service incident, appropriate Agency IT personnel and the ISO should be notified immediately. Any source of information that may provide additional insight into the incident should be reviewed and secured. These include but are not limited to the following: User notifications, Web Application Firewall (WAF) alerts and logs, ISP notifications, intrusion detection system (IDS) logs, firewall logs, netflow data, system logs, SIEM logs and alerts, and notifications by other third parties.

Evaluate the information gathered and determine if an incident response process is to be initiated.

At the outset of an incident the following information is to be documented. This represents the minimum information:

- Incident date and time, including time zone;
- Person reporting incident;
- System/Network owner information including name, business unit and phone number;
- System/Network Function (e.g., web server, external e-commerce network, etc.);
- System IP Address, hostname, and agency asset tag number;
- Operating System, including version, patches, etc. (may be obtained from agency asset management or other system configuration data sources); and
- Method used to identify the incident (e.g., ISP, MSSP, IPS/IDS, network personnel, audit log analysis, system administrator).

Notify the System and Network Administrator(s) of the impacted system(s)/network(s).

DETECTION & ANALYSIS

The below table lists some malicious actions and corresponding indicators of possible DoS attacks against agency networks and systems. While these indicators may allow the agency to respond to a DoS attack, benign and malicious activity often present similar symptoms. For example, users may report a system as being unavailable and an investigation might show that network connectivity was lost. As such, incident responders will need to differentiate between malicious and benign activity before declaring the unavailability of a system, application, service or network as a cybersecurity incident.

Malicious DoS Activity	Indicators
Network-based DoS against a particular system	• User reports of system unavailability • Unexplained connection losses • Alerts from MSSP, IDS/IPS and/or WAF • Network intrusion detection alerts • Host intrusion detection alerts • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Alerts from ISP, IPS/IDS, MSSP, and/or WAF • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses • Reports from ISPs or MSSPs

DoS attacks pose some additional challenges in terms of incident analysis:

- DoS attacks often use connectionless protocols (UDP and ICMP) or use a connection-oriented protocol in such a way that full connections are not established (e.g., sending TCP SYN packets to create a synflood attack). Therefore, it is relatively easy for attackers to use spoofed source IP addresses, making it difficult to trace the source of attacks. ISPs may be able to assist in tracing the activity, but it is often more effective to review logs for previous reconnaissance activity that appears to be related. Because the attacker would want to receive the results of the reconnaissance, such activity is unlikely to use a spoofed address, so it may indicate the location of the attacker.

- DDoS attacks often employ thousands of systems that are controlled by a single handler (or no handler at all). These systems usually have bots installed that are considered "zombies" and are activated by the controller to attack other systems. Agencies will not see the IP of the handler.

- Network-based DoS attacks are difficult for IDS/IPS sensors to detect with a high degree of accuracy. For example, synflood alerts are one of the most common false positives in network IDS/IPS systems. If an attacker performs a rapid SYN scan, many IDS/IPS systems will report it as a synflood, even though the activity is sending only one request to each port. If a server crashes, systems trying to reconnect to it may keep sending SYN packets. Sometimes many legitimate connections in a short time (e.g., retrieving many elements of a Web page) will also cause a synflood alert to be triggered.

The following table provides incident responders with information related to the types of traffic that may be included in DoS/DDoS attacks against SONJ.

Traffic Type	Description
HTTP Headers	HTTP headers are fields which describe which resources are requested, such as URL, a form, JPG, etc. HTTP headers also inform the web server what kind of web browser is being used. Common HTTP headers are GET, POST, ACCEPT, LANGUAGE, and USER AGENT. The requester can insert as many headers as they want and can make them communication specific. DDoS attackers can change these and many other HTTP headers to make it more difficult to identify the attack origin.
HTTP POST Flood	An HTTP POST Flood is a type of DoS attack in which the volume of POST requests overwhelms the server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server.
HTTP POST Request	An HTTP POST Request is a method that submits data in the body of the request to be processed by the server. For example, a POST request takes the information in a form and encodes it, then posts the content of the form to the server.
HTTPS POST Flood	An HTTP POST Flood is a type of DoS attack in which the volume of POST requests overwhelms the server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server. An HTTPS POST Flood is an HTTP POST flood sent over an SSL session. Due to the use of SSL it is necessary to decrypt this request in order to inspect it.
HTTPS GET Flood	An HTTPS GET Flood is an HTTP GET flood sent over an SSL session. Due to the SSL, it is necessary to decrypt the requests in order to mitigate the flood.

Traffic Type	Description
HTTPS GET Request	An HTTPS GET Request is an HTTP GET Request sent over an SSL session. Due to the use of SSL, it is necessary to decrypt the requests in order to inspect it.
HTTP GET Flood	An HTTP GET Flood is a layer 7 application layer DoS attack method in which attackers send a huge flood of requests to the server to overwhelm its resources. As a result, the server cannot respond to legitimate requests from the server.
HTTPS GET Request	An HTTP GET Request is a method that makes a request for information from the server. A GET request asks the server to give you something such as an image or script so that it may be rendered by a browser.
SYN Flood	SYN Flood works by establishing half-open connections to a node. When the target receives a SYN packet to an open port, the target will respond with a SYN-ACK and try to establish a connection. However, during a SYN flood, the three-way handshake never completes because the client never responds to the server's SYN-ACK. As a result, these "connections" remain in the half-open state until they time out.
UDP Flood	User Datagram Protocol (UDP) floods are used frequently for larger bandwidth DoS attacks because they are connectionless and it is easy to generate UDP messages.
ICMP Flood	Internet Control Message Protocol (ICMP) is primarily used for error messaging and typically does not exchange data between systems. ICMP packets may accompany TCP packets when connecting to a sever. An ICMP flood is a layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.
MAC Flood	A rare attack, in which the attacker sends multiple dummy Ethernet frames, each with a different MAC address. Network switches treat MAC addresses separately and hence reserve some resources for each request. When all the memory in a switch is used up, it either shuts down or becomes unresponsive. In a few types of routers, a MAC flood attack may cause these to drop their entire routing table, thus disrupting the whole network under its routing domain.

CONTAINMENT, ERADICATION & RECOVERY

Containment for a DoS incident usually consists of stopping the DoS attack. Sometimes this is easy; usually it is not. Often the first thought is to block all traffic from the source of the activity. However, as previously mentioned, such attacks often have spoofed source addresses or use thousands of compromised "zombie" systems - in either case, making it difficult or impossible to implement effective filtering based on source IP addresses. Even if agency network administrators can block the source addresses that are being used, the attacker can simply move to other IP addresses.

Mitigating DoS attacks is most effective as part of the Preparation stage by implementing solutions to prevent agencies from being impacted by a DoS attack. If not implemented in the preparation phase, then the following solutions may be used to contain, eradicate and recover from a DoS attack.

Filtering Implemented by ISP

A network-based DoS from external hosts will likely overwhelm OIT's Internet routers. As such, OIT network engineers should work with its ISPs to implement filtering of unnecessary protocols upstream from the routers. Typically, this includes blocking UDP and ICMP traffic.

At a minimum, firewalls should be set to with thresholds for ICMP and UDP flood screening.

Enable Rate Limits
Agencies should consider employing a Content Delivery Network and Web Application Firewall (WAF) to distribute content and protect agency web sites from malicious traffic. Enabling HTTP and HTTPS rate limits will block systems from overwhelming agency systems.

Similarly, enabling rate limits at agency firewalls can help mitigate the effects of a DoS attack, for example limiting the number of SYNs per IP per second. Routers adjacent to the firewalls should also be configured to rate limit traffic.

Correct the Vulnerability or Weakness That Is Being Exploited
If the attack can occur because packet filters do not block packets using UDP port 7 (echo), and a publicly accessible host is accidentally running echo, the filters should be altered to block packets destined for the echo port; and the system's configuration should be changed so that it no longer offers the echo service. If an unpatched operating system is susceptible to a DoS from specially crafted packets, then a patch of the operating system is necessary. The system may need to be temporarily disconnected from the network to halt the DoS while the host is strengthened.

Relocate the Target
If a particular system is being targeted and other containment strategies are not working, the target system could be moved to a different IP address. This is deemed "security through obscurity" because the attacker may locate the moved target and attack it again. The targeted service could be transferred to a different host—one without the same vulnerability.

The same solutions and actions taken to contain a DoS attack are the same actions that are used to eradicate and recover from an attack.

POST INCIDENT ACTIVITIES
Ensure solutions used to recover from the attack are implemented across all Departments' and Agencies' systems and/or web sites.

Document the details of the incident and the steps taken to neutralize the incident and determine the root cause of the infection.

Perform an analysis of the following areas to determine where performance could have been improved:

- Whether preparation was adequate;
- Whether detection was prompt and response procedures were adequate;
- Whether the incident was sufficiently contained;
- Whether recovery was adequate; and
- Whether personnel and organization communications were adequate throughout the response to the incident

Submit any recommendations for enhanced computer security processes.

Complete the Closing Memorandum and submit to the ISO and the NJCCIC for review. The Closing Memorandum will be distributed by the ISO to only those with a need to know.

ATTACK POSSIBILITIES BY OSI LAYER						
OSI Layer	**Protocol Data Unit (PDU)**	**Layer Description**	**Protocols**	**Examples of DoS Techniques**	**Potential Impact of DoS**	**Mitigation Options**
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer.	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks.
Presentation Layer (6)	Data	Translates the data format from sender to receiver.	Uses the Protocols Compression & Encryption	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server.	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in

						protected memory on a secure bastion host.
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on).	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable.	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3.	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service.
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP	Can affect available network bandwidth and impose extra load on the	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance.

				messages to overload the targeted network's bandwidth.	firewall	
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer.	Uses the Protocols 802.3 & 802.5 and its devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered.
Physical	Bits	Includes, but not limited to, cables, jacks, and hubs	Uses the Protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets.

8.5 HANDLING A DATA BREACH INCIDENT

Departments and Agencies of the Executive Branch of State Government provide services to the citizens of New Jersey. Often time that includes collecting, processing, storing, and transmitting Personal Information of individuals. While we continue to work to protect our systems and remain vigilant to new threats, we are also cognizant of the fact that achieving 100% security is not possible. As such, an agency's response to a data breach must ensure it is handled responsibly and quickly, and with our citizen's and employee's best interests they are always top-of-mind.

What is a Data Breach

A data breach is a compromise of the security, confidentiality, or integrity of, or the loss of agency computerized or hard copy (paper) data that results in, or there is a reasonable basis to conclude has resulted in:

- The unauthorized acquisition of Sensitive Personally Identifiable Information; or
- Access to Personal Information that is for an unauthorized purpose, or in excess of authorization.

Due to the severity of a data breach, it is categorized separately as a Cat 7 incident. Data breaches are always considered high severity incidents.

Reporting a Data Breach

OIT shall immediately report a data breach to the NJCCIC in accordance with the NJ Identity Theft Prevention Act which states:

Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

To meet this statutory requirement, breaches may be reported to the NJCCIC via email databreach@cyber.nj.gov or by telephone: 1-833-465-2242 or OHSP CT Watch: 1-866-472-3365

The NJCCIC will notify the New Jersey State Police Cyber Crimes Unit and the Office of the Attorney General for legal counsel and guidance in determining the agency's notification responsibilities and response process.

When Notification Is Required

There are many factors that determine an agency's notification responsibilities and requirements. They include the type of information breached, the individuals who may be impacted by the breach, the impacted individuals' jurisdictions, and other legal, regulatory, and contractual requirements.

The following incident examples may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to Personal Information maintained by an agency in either paper or electronic form.

- A user (employee, contractor, or third-party provider), with authorized access to personal information, accesses, copies, or otherwise misuses it thereby compromising the confidentiality of the information.
- An intruder has broken into an agency's database(s) that contains individual(s) personal information.
- Computer equipment, such as a workstation, laptop, tablet, USB drive, or other electronic media containing personal information has been lost or stolen.
- An agency has not properly disposed of records containing an individual(s) personal information.
- A third-party service provider has experienced any of the incidents described above.

The following incidents may not require notification to individuals under applicable laws and regulatory requirements or contractual commitments (provided the agency can reasonably conclude that the misuse of the information is unlikely to occur).

- The agency is able to retrieve Personal Information that was lost, stolen or accessed without authorization, and based on the investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The agency determines that an individual(s) personal information was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.
- An intruder accessed files that contained only individuals' names and addresses.
- A laptop computer is lost or stolen, but the data is encrypted and can only be accessed with a secure password.

Questions regarding what constitutes a breach and notification obligations may be directed to the NJCCIC, the NJSP Cyber Crimes Unit, and/or the Office of the Attorney General.

This Cybersecurity Incident Response Plan outlines steps to take upon discovery of a data breach. There are many facets of a data breach that require the agency to act quickly and effectively in an effort to not only contain the breach and provide protection to affected individuals, but to also protect the agency from legal, regulatory, financial, and reputational harm. While a data breach may result from a vulnerability in an IT system, network, or service that was exploited, the agency's response to the breach extends far beyond the remediation of the technical weakness. As such, CSIRT members responding to a breach may include the NJSP Cyber Crimes Unit, the NJCCIC, the Office of the Attorney General, the Public Information Office, Human Resources, and other internal resources as necessary. Additionally, external service providers including data breach response services, outside counsel, public relations, data breach service providers and computer forensics firms, and federal law enforcement may be required to assist in handling data breaches and other high severity Cybersecurity incidents.

A data breach is most often the result of a preceding Cybersecurity incident such as unauthorized access or malicious code. The discovery of the breach may be made as a result of the response efforts when handling these incidents. Often times, breaches go undetected and an agency may only become aware of the breach after receiving a report by employees, contractors, banks, media, law enforcement, or other third parties.

The facts discovered during the CSIRT's response to a Data Breach incident will determine the necessary response activities. The following checklist (under "Initial Action" below) is presented as a guide (as opposed to a strict sequence of actions to be followed). During all phases of the response, the CSIRT will ensure all actions and findings are documented and will communicate with the appropriate stakeholders.

INITIAL ACTION

Upon a report of a Data Breach incident, the agency ISO, Agency Head, and the NJCCIC should be notified immediately. Any sources of information that may provide additional insight into the incident should be secured. These include, but are not limited to, the following: information received from the reporter of the incident, SIEM console alerts, email notifications, intrusion detection system (IDS) logs, firewall logs, netflow data, system access logs, etc.

At the outset of an incident the following information is to be documented. This represents the minimum information:

- Incident date and time, including time zone;
- Person reporting incident;
- System owner information including name, business unit and phone number;
- System Function (e.g., web server, database server, workstation, etc.);
- System IP Address, hostname, and agency asset tag number;
- Operating System, including version, patches, etc. (may be obtained from agency asset management system or other system configuration data sources);
- Antivirus software installed, including version, and latest updates;
- Attacker's IP, hostname, port, and protocol; and
- Method used to identify the incident (e.g., IDS, audit log analysis, system administrator, third party reporter)

Notify the System Administrator(s) or Custodian(s) of the breached system(s) and instruct them to not to use, modify or power off the system(s) until directed by appropriate CIRT personnel.

DETECTION & ANALYSIS

Once a Data Breach has been confirmed many of the CIRT activities will occur in parallel. The Director of the NJCCIC or a designee will act as the Incident Coordinator to ensure all necessary response activities are carried out by the respective CIRT members.

The Director of the NJCICC or a designee will notify the NJSP Cyber Crimes Unit, the Office of the Attorney General, the State CTO, OIT CISO, the Director of the Office of Homeland Security and other members of the ISGC to provide them with an overview of the incident. The Office of the Attorney General will assess whether there is a notification requirement.

Since a response to a Data Breach will involve many members of the CSIRT, the activities in each phase of the response have been organized according to functions.

Agency IT, Agency Information Security, NJSP Cyber Crimes Unit, NJCCIC, and OIT Personnel: Determine the type of Personal Information(PII) that may have been compromised, including but not limited to:

Name, Address, SSN, DOB, Driver's License Number, Financial Account Number, Cardholder Data, Protected Health Information, email address, username, password, PIN, etc.

Determine where and how the breach occurred.

Identify the source of compromise, and the timeframe involved.

Review the network logs and flow data to identify all compromised or affected systems.

Consider third party and extranet connections, the internal agency local area and wide area networks, test and production environments, and virtual private networks. Look at appropriate system and audit logs for each type of system affected.

Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

The following list includes some of the volatile information that should be collected from the victim system(s) prior to powering down:

- System Date, Time, Time zone
- System Information Summary
- Audit Policy
- ARP Cache
- DNS Cache
- NetBIOS Name Table
- Routing Table
- Current Network Connections
- Running Processes
- Running Services or Daemons
- System, Application, and Security Logs
- The System Registry
- Scheduled Jobs
- Program Started at Boot or User Login
- Users Currently Logged In
- Files Open over the Network
- Open TCP/UDP Ports
- IP Configuration
- Hidden Files/Alternate Data Streams
- Protected System Files
- Various Root Kit Detection Profiling
- Full Memory Dump
- Swap/Tmp File Dump
- Hibernation File Dump
- Dump of Suspicious Processes Running in Memory

Examine all volatile information as well as all logs obtained to determine the level of compromise (user, root or data). Look for altered malware, system files, added programs, root kits, Bot Nets, back-doors, hidden special files and directories.

Determine the scope of compromise by examining network records for potential access to other systems within the agency and other agencies from the compromised system. If more systems are found to have been accessed, run the above identification steps for each suspect system.

Create a forensics image of the impacted system(s) and run forensic analysis to determine the details of the type and nature of the compromise.

Office of Attorney General
Upon confirmation of a Data Breach, determine notification requirements, provide legal guidance and counsel, and engage outside legal counsel, if appropriate.

If the breach occurred at a third-party location, determine if a legal contract exists and review contract terms.

CONTAINMENT, ERADICATION AND RECOVERY

Agency IT, Agency Information Security, NJSP Cyber Crimes Unit, NJCCIC, and Office of Information Technology (OIT)
Carry out all Containment, Eradication and Recovery functions included in a Cat 1 – Unauthorized Access incident response. Additionally:

- Take measures to contain and control the incident to prevent further unauthorized access to or use of Sensitive PII, including shutting down particular applications or third-party connections, reconfiguring firewalls, and modifying physical access controls.
- Change all applicable passwords for UserIDs that have access to Sensitive PII, including system processes and authorized users. If it is determined that an authorized User's account was compromised and used by the intruder, disable the account.
- Monitor systems and the network for signs of continued intruder access.
- Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the evidence is collected in a forensically sound manner. Document all actions taken, by whom, and the exact time and date.

Each CSIRT member involved in the response must record his or her own actions. Record all forensic tools used in the investigation.

If it is determined that the attacker is originating from an external host/network and the attack is escalating, disconnect or block the attacker at the perimeter firewall.

If the compromise is spreading to other systems escalate the incident to appropriate CSIRT members and consider disconnecting impacted systems to contain the threat.

Ensure that all system processes related to the compromise have been stopped and removed from the system.

Run a full vulnerability scan of the compromised system(s) and submit the scan report to the System Administrator(s) for remediation.

Ensure that all files modified or added to the system by the attackers have been removed.

If the compromise was determined to be at a system or root level the system should be wiped and the operating system reinstalled and hardened to prevent a reoccurrence.

Review and restore any affected data modified or deleted from backups, if possible. If the data files are contaminated (i.e. macro virus) ensure they are cleaned before restoring.

Review system configurations to ensure the following are current:

- Versions and patches of all system software;
- Auditing and monitoring of systems;
- System and data access control lists; and
- User/System accounts

Rerun a vulnerability scan on the system(s) to ensure all known issues have been remediated.

Ensure all actions are documented and communicated to relevant stakeholders.

Monitor access to database files and repositories that contain Sensitive PII to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).

Identify individuals whose information may have been compromised. An assumption could be "all" if an entire database table or file was compromised.

Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.

Upon request from the Incident Coordinator, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

Office of Attorney General
Provide advice, counsel, direction and investigative support throughout all aspects of the agency's response to a Data Breach.

Engage and act as the primary point of contact for outside legal services.

Provide guidance throughout the investigation on issues relating to privacy of personal information.

Assist in developing appropriate communication to impacted parties.

Coordinate with the Public Information Office and the Incident Coordinator on the timing and content of notification to impacted parties, including individuals, banking institutions, etc.

If necessary, notify the appropriate authorities (e.g., other States Attorneys General Offices, Federal Trade Commission (FTC), etc.).

Public Information Office
Act as the primary media contact.

Coordinate and develop appropriate internal and external communications with OAG and Human Resources, as necessary.

Engage and act as liaison with external communications and public relations firms.

Track and monitor media coverage, including social media, and respond as appropriate.

Human Resources
If warranted, work with the OAG and the Public Information Office to develop and provide relevant information and direction to associates and contractors.

Act as primary liaison for employee and contractor inquiries.

Document all inquiries and contacts related to the Data Breach.

POST INCIDENT ACTIVITIES
Update monitoring signatures and/or escalate alert responses to prevent a reoccurrence of the incident.

Document the details of the incident and the steps taken to neutralize the incident and determine the root cause.

Perform an analysis of the following areas to determine where performance could have been improved:

- Whether preparation was adequate;
- Whether detection was prompt and response procedures were adequate;
- Whether the incident was sufficiently contained;
- Whether recovery was adequate; and
- Whether personnel and organization communications were adequate throughout the response to the incident.

Submit any recommendations for enhanced computer security processes.

Complete the Closing Memorandum and submit to the OIT CISO and State CISO for review. The Closing Memorandum will be distributed to only those with a need to know.

While the incident response process for a data breach may be completed after a recovery from the incident and the submission of a Closing Memorandum, there will likely be ongoing activities from various CSIRT members, including the OAG, Public Information, the NJSP, the NJCCIC, OIT and the agency IT and Information Security functions.

9 APPENDIX A: DATA BREACH NOTIFICATIONS AND COMMUNICATIONS

The following section provides guidance regarding the notification and communications that may be required as a result of a Data Breach. In most states in the USA, once the compromise of Personal Information(PII) is confirmed to be a breach, a notice to affected individuals must be sent without unreasonable delay. This section includes guidance on notifications and example communications. The facts discovered during the CSIRT's response to a Data Breach incident will guide the agency as to the necessary notification and communications requirements.

All notifications and communications regarding a Data Breach must be approved by the Office of the Attorney General and the Public Information Office, as necessary to communicate or notify individuals and the various constituencies for which notification is required.

9.1 Notification to Affected Individuals

To the extent warranted and required by law, or at agency's discretion, the OAG working in conjunction with the Public Information Office and other members of the CSIRT will promptly:

- Identify and notify affected individuals; or
- If the affected individuals cannot be identified, the OAG or its designee will determine the groups likely to have been affected, and will notify those individuals in the groups likely to have been affected; and
- The agency will send notice to all affected individuals living in states where breach notification is mandated.

Notice to impacted individuals should be consistent with laws and regulations the agency is subject to. The Office of Attorney General will maintain an up-to-date list of applicable laws in each state.

Appropriate delivery methods include:

- Written notice;
- Email notice; and/or
- Substitute notice
  - Conspicuous posting of the notice on the agency's or the State of NJ's websites.
  - Notification to major media

Depending on the scope and size of the Data Breach, the CSIRT may decide to engage a Data Breach Service Provider to assist with notifications.

The notice to impacted individuals should include the following:

- a general description of the incident;
- information to assist individuals in mitigating potential harm
  - including a customer service number,
  - steps individuals can take to obtain and review their credit reports and to
  - file fraud alerts with nationwide credit reporting agencies,
  - sources of information designed to assist individuals in protecting against identity theft;
  - remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft.

- Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft and encourage the individual to report any suspected incidents of identity theft to the FTC.

- Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected incidents of identity theft. At the time of this document's publication, the website address is http://www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-IDTHEFT.

9.2 Timing of Notification to Affected Individuals

Once the CSIRT has reason to believe that a breach of Sensitive PII is reasonably likely to have occurred, the OAG will arrange for the provision of notice to affected individuals without unreasonable delay, unless:

- The NJSP Cyber Crimes Unit or other law enforcement authorities determine that providing notice at such time would impede their investigation, or
- The agency is taking measures necessary to determine the scope of the breach and restore the reasonable integrity of the affected system(s), in which case notice will be made as soon as reasonably practicable thereafter.

9.3 Notification to the New Jersey State Police

Upon suspicion of a Data Breach incident the agency shall notify the NJCCIC without delay. The NJCCIC will in turn notify the NJSP Cyber Crimes Unit and the OAG. The NJCCIC will also escalate notifications as appropriate.

NJSP Cyber Crime Unit and OAG officials will confer to determine if the agency may proceed with notifying impacted individuals. If the agency is informed that giving notice may impede a criminal investigation, then notification to individuals may be deferred.

9.4 Notification to States

To the extent warranted and required by law the OAG or its designee will promptly provide written notice of a Data Breach to the relevant state governmental authorities (in the USA). Such notification will provide information as to the:

- Nature and circumstances of the breach;
- Timing, content, and distribution of the notices; and
- Approximate number of affected individuals of that state or province.

9.5 Notification to Federal Data Sharing Partners - IRS and SSA

If an identified Data Breach involves the Internal Revenue Service's Federal Tax Information (FTI) or the Social Security Administration's Personally Identifiable Information (PII), NJOIT shall immediately notify and collaborate with the impacted NJ State agencies, and the IRS and SSA shall be notified, as follows:

Requirements	IRS	SSA
What is considered a data incident?	A data breach occurs if **FTI is improperly disclosed, used, accessed, or handled** in a way that violates security or confidentiality requirements. Examples include: • Unauthorized access to FTI by employees, contractors, or external parties • Loss or theft of physical or electronic records containing FTI • Cyberattacks, including ransomware, phishing, or hacking incidents affecting FTI • Improper disposal of FTI (e.g., failing to shred sensitive documents) • Sending FTI to unauthorized recipients via email, mail, or other methods	A data breach occurs if SSA data is: • **Accessed by unauthorized individuals** (e.g., hackers, employees without need-to-know access). • **Lost, stolen, or improperly disclosed** (e.g., sending data to the wrong recipient). • **Used improperly or for unauthorized purposes** (e.g., identity theft, fraud). • **Modified or destroyed without authorization.** • **Compromised due to cyberattacks**, including ransomware, phishing, or malware. • **Stored, transmitted, or handled insecurely**, exposing it to potential unauthorized access.
When to notify?	Immediately, or no later than **24 hours** of detection.	Within 1 **hour** of detection
Who to call?	When an unauthorized disclosure or data breach occurs, the agency must not wait to conduct an internal investigation to determine if federal tax information (FTI) was involved. If FTI may have been involved, the agency must contact: Office of Safeguards by email to the Safeguards mailbox, safeguardreports@irs.gov The Office of Safeguards will determine if the incident meets the criteria to be reported to the Treasury Inspector General for Tax Administration (TIGTA). If so, the IRS Office of Safeguards will contact TIGTA at **1-800-366-4484.**	SSA Regional Office and SSA Systems Security Contacts: **Lauren Hsu** Phone: (212) 264-8355 Email: Lauren.Hsu@ssa.gov **Cheyla P. Ocasio** Phone: (212) 264-7317 Email: Cheyla.P.Ocasio@ssa.gov **Elizabeth Roback** Phone: (212) 264-3455 Email: Elizabeth.Roback@ssa.gov **Donald Scott** Phone: (410) 965-8850 Email: Donald.Scott@ssa.gov **Angil Escobar, Branch Chief** Phone: (410) 965-7213 Email: Angil.Escobar@ssa.gov **Steven Harkness** Phone: (410) 966-5971 Email: Steven.Harkness@ssa.gov If the above contacts are not reachable: **SSA's National Network Service Center** at 1-877-697-4889 If National Network Service is not reachable: **SSA's Office of Information Security, Security Operations Center** at 1-866- 718-6425

Requirements	IRS	SSA
What information to report?	To notify the IRS Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including, but not limited to: • Name of agency and agency Point of Contact information for resolving data incident • Date and time the incident occurred • Date and time the incident was discovered • How the incident was discovered • Description of the incident and the data involved, including specific data elements, if known • Address where the incident occurred and Information technology equipment involved (e.g., laptop, server, mainframe)	NJOIT is the **State Transmission Coordinator (STC),** responsible for overseeing the secure transmission of data between NJ State agencies and the SSA. Full details of what information to report are contained in Attachment C to the SSA/NJOIT STC Agreement. High-level categories: 1. Information about the individual making the report to the SSA. 2. Information about the data that was lost/stolen. 3. How was the data physically stored, packaged, and/or contained? 4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the SSA, information about this employee/contractor. 5. Circumstances of the loss. 6. Have any other SSA components been contacted? If so, who? 7. Which reports have been filed? 8. Other pertinent information.

9.6 Notification to Payment Card Issuers and Banks

While the State of New Jersey outsources card payment services to a third-party provider and the third-party shall notify the Treasury Department of a breach of its systems, there may be instances where agency systems, databases, and other data repositories store cardholder data. In instances in which cardholder data associated with a credit or debit card is reasonably believed to have been acquired or accessed by an unauthorized person, the OAG and/or the Treasury Department will notify the relevant payment card issuers and banks in accordance with credit card companies' and banks' specific contractual requirements for reporting suspected or confirmed breaches of cardholder data.

The following references (or their latest version equivalents) should be consulted for specific requirements.

- American Express Data Security Operating Policy for Canadian Merchants, Aug 2010
- What To Do If Compromised, Visa Inc. Fraud Control and Investigations Procedures, v. 4.0, September 2013
- Account Data Compromise User Guide, MasterCard, June 2014

The table below summarizes high level notification requirements for some of the card issuers.

Requirements				
What is considered a data incident?	Suspected or confirmed access, use, loss, theft, or misappropriation of credit card data.	Not specified	An incident involving at least one MasterCard account number in which there is unauthorized access or use of cardholder data or sensitive authentication data.	Access, use, loss, theft, or misappropriation of credit card data.
When to notify?	Within 24 hours following the discovery of a data incident	Not specified	Immediately following the discovery of the incident.	Within 24 hours following the discovery of the incident.
Who to call?	888-732-3750 (US only) 602-537-3021 (Canada)	Not specified	MasterCard Alerts and ADC Reporting Form online system	Agency's acquiring bank or 650-432-2978 (US only) 416-860-3090 (Canada)
When we need to use a Qualified Incident Response Assessor (QIRA)?	Required for data incidents involving 10,000 cards or at AMEX request	Not specified	Engage within 3 days of incident Notify MC within 2 days, that the QIRA was engaged	If necessary, it will be specified by Visa

9.7 Coordination with Credit Reporting Agencies

The OAG or the Treasury Department will contact the following consumer credit reporting agencies as required:

Credit Reporting Agencies

Experian	Equifax	TransUnion
Experian Security Assistance P.O. Box 72 Allen, TX 75013 Tel.: 1-888-397-3742	Equifax Information Services, LLC Office of Consumer Affairs 1550 Peachtree St. Atlanta, Georgia 30309 Tel.: 1-800-525-6285 Direct Dial: 678-795-7944	P.O Box 6790 Fullerton, California 92834 Tel.: 1-800-680-7289 Fax: 714-680-7290

9.8 Public Notification

In the event the CSIRT in consultation with the OAG determines public notification of a breach is warranted, the Public Information Office with assistance from the OAG will disseminate appropriate public notices and handle all media inquiries.

9.9 Crisis Communication Guide

Contents

To assist you in your conversations, this guide contains:

- Overview
- Agency Media Protocol
- Key Messages
- Q&A document for affected employees and individuals

Overview

The purpose of this document is to help you manage communication with your employees and the individuals your agency provides services to regarding a report of a data breach/incident at your agency. This toolkit contains a sample media protocol, key messages and a Q&A document for your reference.

Please note: All leaders are accountable for conveying the message in accordance with this toolkit and ensuring that their team receives and understands the key messages.

While this sample guide does not include answers to all of the questions that might be asked, it provides you with the general information that is available so you can support your team and continue to serve your agency's customers.

This announcement may be reported by the media, making it important for you to spend time talking with your employees so they understand what this means, what will happen next and how they will be affected.

Please DO NOT distribute or post any of the contents contained in this toolkit. You can rely on your HR partners for support during this time.

MEDIA PROTOCOL: If you or any of your employees are approached by the media, please direct them to your Public Information Office. If you are contacted by a member of the media, please refer to SONJ's media protocol below.

9.10 OIT Media Protocol

The OIT Office of Communications and Digital Services is responsible for ensuring all information and messaging about the Agency is consistent and supports the Agency's and the State's positioning.

IMPORTANT NOTE: agency employees and contractors, including managers, should not offer any opinion to the media regarding the Agency's or the State's position on any issue. Keep in mind the media is not obligated to identify themselves.

Please direct any media inquiries to:
Julie Garland Veffer | Director, Communications & Digital Services | NJ Office of Information Technology | o: 609-815-2140 | Julie.Veffer@tech.nj.gov

Example of an employee's response to a media call or to media entering the Agency's facilities or offices:

"Thank you for your interest. Can I transfer you to someone from our Public Information Office who can better answer your questions?"

Media entering Agency premises:
In the event that broadcast media show up, you should politely inform them that the Agency policy does not allow media inside without prior approval and ask them to contact the Agency's Public Information Office directly regarding their request for information. They may try to get you to answer questions on the spot. In this case, simply reinforce that you are not an Agency spokesperson and as such, ask them to contact the Agency Public Information Office.

9.11 Key Messages to Assist You in Conversations with Your Teams

- Today we received a report of a data breach/incident across in our Agency.
- At this time, we are working to determine the extent of the incident and how individuals have been affected.
- We are currently investigating to determine the precise timeline of events.
- The privacy and security of our employees and the general public who entrust us with their data is of utmost priority and we are taking this matter extremely seriously.
- We have implemented our response plan, which places the highest priority on the safety and security of the public and our employees.
- We are working with law enforcement and other parties to investigate the issue and protect the public and our employees.
- We are moving quickly and aggressively to resolve this issue and are committed to open and transparent communication with our employees and the public throughout this process.
- We will continue to keep you updated as we progress and as more information becomes available.

9.12 FAQs

The following are sample answers to help manage many of the questions agencies may receive from employees and/or the general public.

While these do not represent all of the questions that might be asked, it provides agencies with the general information that is available so they can support their teams and continue to serve the public. Agencies can rely on their HR representatives for support during an incident.

9.12.1 Employee Sample Q&A

1. What has happened - have we confirmed a breach?

   A: On (date) we learned that unauthorized individuals had (e.g.: illegally accessed <agency> systems and obtained <employee/individual PII/SPII). This is an ongoing investigation, however, at this time we are able to confirm that (e.g.: the information that was accessed includes <data types (e.g. names, mailing addresses, email addresses or phone numbers)>.

2. What information was compromised/ stolen?

   A:

3. How many individuals were affected by this

   incident? A:

4. Were employees also affected by this incident?

   A:

5. What are we doing to resolve this issue?

   A:

6. How do I find out if I was affected?

   A:

7. Has the issue been resolved?

   A: We continue to move quickly and aggressively to resolve this issue. We are working around the clock with law enforcement, and others to investigate the issue and protect the general public and our employees.

8. When did we become aware our systems were compromised?

   A:

9. Who are we working with to investigate?

   A:

10. What are we doing to ensure an incident of this kind does not happen again?

    A: We take our employees'/general public's privacy and security very seriously, and we are constantly enhancing our systems and processes. We are currently examining what additional measures we can take to ensure the privacy and security of our customers' information and prevent any future incidents of this nature.

9.12.2 General Public Sample Q&A

1. Have you confirmed a breach? What information was compromised/ stolen?

   A: On (date) we learned that unauthorized individuals had (e.g.: illegally accessed <agency> systems, and obtained < general public PII/SPII>. This is an ongoing investigation, however, at this time we are able to confirm that (e.g.: the information that was accessed includes <data types (e.g. names, mailing addresses, email addresses or phone numbers)>.

2. How many individuals were affected by this incident? How do I know if I was affected?

   A:

3. Has the issue been resolved?

   A: We continue to move quickly and aggressively to resolve this issue. We are working around the clock with law enforcement, and others to investigate the issue and protect the general public and our employees.

4. When did you become aware your systems were compromised? When did the investigation begin?

   A:

5. What are you doing to ensure an incident of this kind does not happen again?

   A: We take our employees'/general public's privacy and security very seriously, and we are constantly enhancing our systems and processes. We are currently examining what additional measures we can take to ensure the privacy and security of our customers' information and prevent any future incidents of this nature.

6. Can I still use my credit card, or should I have a new one issued? A:

7. If I used my debit card or credit card on a State website or in a State agency, was my information compromised/stolen?

   A:

8. What does it mean if my information was stolen? What are the risks to my safety and security?

   A:

9. What can I do to protect myself from fraudulent charges/ identity theft?

   A: It is a good idea to review your payment card statements carefully and call your bank or credit card issuer immediately to report if you see any suspicious transactions.

10. I believe I have fraudulent charges on my credit/debit card. Will I be held liable for these charges?

A: You will not be responsible for any fraudulent charges. The financial institution that issued your card or the State of NJ will assume responsibility for those charges. If you have not already done so, you should report any suspicious transactions to the financial institution that issued your card in a timely manner.

9.13 AGENCY SAMPLE BREACH NOTIFICATION LETTER

Below is a sample breach notification letter that may be tailored to the facts of a Data Breach. The Office of the Attorney General and the OIT Office of Communications & Digital Services are responsible for drafting all notification letters and other communications pertaining to a Data Breach.

<Individual Name>
<Street Address>
<City, State Postal Code>
<Date>

Dear <Individual Name>:
We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that <may involve/involves> your personal information.

[Summary of Incident]
<Between/On> <Identify Time Period of Breach>, <Summarize Breach Incident>. The data accessed <may have included/included> personal information such as <Identify Types of PII at Issue>. To our knowledge, the data accessed did not include any <Identify Types of PII Not Involved>.

[Actions Taken After Learning of the Breach]
The State of New Jersey values your privacy and deeply regrets that this incident occurred. The State is conducting a thorough review of the potentially affected <records/computer system/others>, and will notify you if there are any significant developments. The <Agency> where the incident occurred has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of the <Agency's> valued <employees/customers/others>. The State has contracted with a leading IT Security company specializing in the investigation and resolution of cyber attacks to help further fortify the protections around your information. The State also is working closely with law enforcement and <other relevant organizations> to ensure the incident is properly addressed.

[Summary of Benefits]
We are offering free identity protection services provided by <Provider>, a leading and trusted identity protection provider, to you for a period of <duration of service> months. This service includes identity theft repair and credit monitoring services. This service is automatically available to you with no enrollment required. If a problem arises, simply call <Provider> at <Toll Free Number> and an investigator will work to recover your financial losses, restore your credit and protect your identity. For further information on the services provided by <Provider> please visit <website of Provider>.. Those without Internet access can call <Toll Free Number>.

In addition, please also review the attachment to this letter (Steps You Can Take to Further Protect Your

Information) for further information on steps you can take to protect your information.

For further information and assistance, please contact <Agency Representative> At <Telephone Number/ Toll-Free Number> between <Time> a.m.- <Time> p.m. <EST> daily, or visit <Website>.

Sincerely,
<Name>
<Title>

9.14 Identity Theft Protection Guidance for Individuals

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, the NJCCIC at cyber.nj.gov, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies Equifax, Experian, and TransUnion once every 12 months. To obtain your free credit report:

- Go to www.annualcreditreport.com;
- Call the toll-free number 877-322-8228; or
- Complete the Annual Credit Report Request Form (available at www.ftc.gov/bcp/conline/includerequestformfinal.pdf) and mail it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

When you receive your credit report, look it over carefully. Look for accounts you did not open and inquiries from creditors that you did not initiate. If you see anything you do not understand call the credit agency at the telephone number provided on the report. Another helpful resource is the Federal Trade Commission's identity theft website at http://onguardonline.gov/idtheft.html or by calling 1-877-IDTHEFT. The Federal Trade Commission can assist victims and potential victims in dealing with the threat of identity theft.

Place a Fraud Alert on Your Credit File
To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert is free and helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take

steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 800-525-6285 www.equifax.com	Experian P.O. Box 1017 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 800-680-7289 fraud.transunion.com

Place a Security Freeze on Your Credit File

You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number or password that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Recently enacted US Federal Law requires that the credit reporting agencies provide security freezes at no cost. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. To place a security freeze you can contact the three credit bureaus at:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	TransUnion Security Freeze P.O. Box 2000 Chester, PA 19022 www.freeze.transunion.com

Lifting a Credit Freeze

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information for Massachusetts Residents

Placing a Credit Freeze: Massachusetts law also allows consumers to place a security freeze on their credit reports. See the description above about what a security freeze does and how to order them with each of the one. Under Massachusetts law, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

Obtaining Police Reports

You have a right to obtain a police report relating to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Additional Free Resources on Identity Theft
You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the Federal Trade Commission to obtain additional information about how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338) | www.ftc.gov/idtheft

A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

For Iowa Residents
You may also contact local law enforcement or the Iowa attorney General's Office to report suspected incidents of identity theft. You can reach the Iowa Attorney General at:

Iowa Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
515-281-5164 | http://www.iowaattorneygeneral.gov.

For Residents of Maryland
You may also obtain information about preventing and avoiding identity theft from the:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place,
Baltimore, MD 21202
1-888-743-0023 | www.oag.state.md.us

For Residents of North Carolina
You may also obtain information about preventing and avoiding identity theft from the:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-919-716-6400 | www.ncdoj.gov

10 APPENDIX B: CYBERSECURITY INCIDENT RESPONSE DOCUMENTATION TEMPLATES

10.1 CYBERSECURITY INCIDENT CONTACT LOG

CSIRT Member:		Incident #:	
Incident Description:			

Date	Time	Person Contacted	Description/Outcome

10.2 EVIDENCE LOG

10.3 POST INCIDENT CLOSING MEMORANDUM

Cybersecurity Incident Response Team
<Date>

To: <ISO/CISO/NJCCIC>

From: <CSIRT Member>

Subject: Closing Memorandum - <Incident #>

The Closing Memorandum contains five sections that together provides a summary the incident and the CSIRT's response.

BACKGROUND:

ACTION TAKEN:

FINDINGS:

CONCLUSION:

EXHIBITS:

Closing Memorandums should be submitted to the OIT ISO no later than 30 days after the conclusion of an incident response.

11 APPENDIX C: Computer Evidence and Forensics Analysis Guide

11.1 Forensic Analysis

The process of forensic analysis of digital evidence incorporates several aspects that are common throughout forensic science. These include:

- Recognition of evidence
- Preservation, collection and documentation
- Classification, comparison and individualization
- Reconstruction

The inherent volatility of digital evidence provides unique challenges to investigators and analysts in handling and analyzing this evidence. Maintaining the integrity of the evidence through safe and proper handling techniques and a documented chain of custody will ensure that the results of a thorough forensic examination and analysis of the digital evidence is irrefutable. Failure to safeguard the evidence from contaminating elements could destroy the integrity of the evidence and thereby produce inaccurate conclusions as a result of a forensic analysis. The documentation of any and all custodial handling of electronic evidence provides a foundation from which the results of an examination and analysis can be verified and reproduced. Each time evidence is handled, the actions performed upon the evidence will be documented in accordance with evidence and control best practices.

Due to the ever-changing technologies associated with digital evidence, these guidelines cannot proscribe to mandate that any one method or set of tools in existence today will be best suited for all cases in the future. Instead, these guidelines are just that - a guide from which a foundation of concepts and principles common to the examination and analysis of all digital evidence can be applied. The principles of image, authenticate and analyze are the precepts upon which SONJ's computer forensics procedures are founded. There are three common methods for a process that includes the collection, authentication and analysis of digital evidence that will be employed. The determination as to which method is to be utilized is dependent on a variety of factors relative to an individual case. Factors that may determine the exact method to be employed for a given instance include legal or jurisdictional issues, technical capabilities, equipment and manpower resources as well as the nature of the case. However, any actions taken during the collection, authentication or analysis of computer evidence will always be documented and reasonable.

The first method for the extraction and analysis of computer-based evidence requires the use of industry standard practices in order to make a "bit-stream" duplicate of media devices where it is deemed necessary to conduct an analysis of the entire data space of the device – including unallocated or slack space. Upon the creation of a "bit-stream" copy, one or more authentication mechanisms will be used to validate the results of the duplication process.

A second method of extracting computer evidence involves investigations whereby it has been determined that the creation of a "bit-stream" image of the evidentiary media is deemed unnecessary and/or outside the scope of the investigation. As with all methods, precautions will be taken to protect the evidence from modifications. In the event that data is copied from the original evidence media, one or more authentication processes will be used to validate the results of the copy process.

A third form of extracting computer evidence entails the processing of computer logs that are maintained by the Agency or other third parties. Such logs include but are not limited to firewall, proxy, mail, file transfer protocol and remote access logs. Often, a third party outside the auspices of the High Technology

Investigations Unit will conduct the processing of such logs. In cases whereby such evidence is to be included, the person accepting this data as evidence will ensure that the third party documents the authenticity of the data and when appropriate, the processes used to extract it.

Due to the rapidly changing nature of technology, the practices and procedures for the forensic analysis of digital evidence may be modified to reflect these advances in technology. The adoption of new methodologies or new technologies for use in the forensic analysis of digital evidence will be predicated upon documentation that these methodologies and/or technologies have met both external and internal scientific testing procedures that meet the respective manufacturer's claims and/or have been accepted as industry standards. Independent testing methods and the results of these tests of third-party hardware and software for use in forensic analysis is to be documented and maintained on file. In addition, other documentation certifying, endorsing and/or attesting to the functionality of this hardware, software and/or forensics methodologies and procedures will also be maintained.

11.2 Bit-Stream Imaging and Authentication

The term "bit-stream" image refers to the process of creating an exact copy of the contents of computer media bit for bit. As such, any bit stream image process should include a copy of all files, directories, partitions, boot records, slack space and unallocated space from a computer media device in a manner whereby the media on which these bits are copied is considered to be an exact duplicate of the media from which the copy was made.

Currently, there are numerous hardware and software products that may be used to achieve the goal of creating a bit-stream image of computer media. These include, AccessData Imager, Guidance Software's Encase, Nuix, OS Forensics; and utilities internal to operating system software such as the "DD" command native to a number of Unix operating systems and its variants. There are other products currently available not mentioned above that also are capable of creating bit-stream copies. No product or method may be used until these products and methods have been verified and documented in the creation of true bit-stream copies of computer media.

Upon the creation of a bit-stream copy there is to be an authentication of the results of the copy process. Authentication may be completed in a number of acceptable ways, including those authentication processes internal to the bit-stream imaging products. Other acceptable methods that should be used in conjunction with any processes to these products include Cyclical Redundancy Checks (CRC); Message Digest MD5 Hash; the revised Secure Hash Algorithm (SHA-2) or other industry acceptable cryptographic one-way hashing algorithms. In instances where a bit stream image is not created, but a file copy is made, the file copy will be authenticated and documented using the same procedures for authentication as listed above. In all cases where computer-based evidence is duplicated, authentication of the duplicate copy will be documented. In cases whereby an analysis of computer-based evidence is conducted on a media device containing original evidence, but where no copy is made, the contents of the media will be benchmarked using a cryptographic hash prior to analysis and then again after analysis to authenticate that no changes were made to the original evidence. These authentications are to be documented and included in the forensic analysis report.

In cases whereby computer evidence has been derived from computer data kept as part of the Agency's normal business practices, and the person(s) submitting this evidence are individuals instructed to retrieve and submit said evidence, the authentication and veracity of this evidence will be documented, and where applicable, the processes used in its retrieval.

11.3 Search, Seizure, and Storage of Evidence

In cases where it is necessary to collect digital evidence, all reasonable precautions to ensure the integrity of the evidence, as well as its chain of custody, to the degree that the evidence will be admissible in judicial proceedings, will be adhered to. These precautions will carry forth from the initial identification of the evidence and through its analysis and storage pending its final disposition. These precautions include limiting any modifications (i.e., additions, deletions and alterations to the contents of computer media as well as the operability and configuration of the evidence seized). Standard practices in the collection and storage of computer evidence will be followed. These practices include the following:

- Storage of evidence in a controlled environment - usually at room temperature and where no foreign elements are introduced that would cause the evidence to become contaminated and/or inoperable. These environmental factors include controls on temperature, humidity or condensation, radio frequencies, magnetic fields, static electricity and other conditions that would contaminate the evidence.

- Computer-based evidence should be handled and transported in a manner such that no damage to any of its components occurs. During its handling and/or transportation, the environmental factors listed in the preceding paragraph should be controlled. Additionally, the materials used to transport computer evidence must be such that no contaminating elements are introduced.

- Evidence that is pending transfer for analysis will be stored in a secure location. Eventually, all evidence is to be transported to, and stored in, a secure location maintained by the Agency. All access to items stored in the secured location will be controlled by the Agency ISO or a designee, who will maintain a log documenting the storage and removal of any evidence in the secure location. The duration of the storage of evidence upon final disposition of the case is to be determined by the State's document retention guidelines.

11.4 On-Scene Logging and Marking of Evidence

During the initial seizure of evidence, all items that are collected should be marked with the incident number, the date and time the evidence was seized, a unique reference number and the initials of the person collecting the evidence. Immediately after seizing and marking the evidence, it will be logged and secured.

11.5 Forensics Analysis Reports

The process of forensic analysis of computer-based evidence results in the extraction and presentation of this evidence into a humanly readable or audible format. Based on the incident facts and the items collected, numerous methods may be employed to extract and present the evidence. Data may be stored on many media types and in many formats and no single analysis method will be capable of extracting and presenting each of these formats. Media will often act as a mere storage device for the data. However, other times the operation of a program stored on a computer or other device will require its operation in conjunction with the device's components in order to document the fact that the evidence is indeed pertinent to the incident. In all cases where a forensic analysis is performed, the forensic analysis technician will concisely document the findings of the analysis in a manner that is admissible at any future proceedings. All forensic analysis reports will document the equipment, software and processes employed to produce the resultant output.

Key Terms and Definitions

Evidence: any of the material items or assertions of fact that may be submitted to a competent tribunal as a means of ascertaining the truth of any alleged matter of fact under investigation before it.

Digital Evidence: encompasses any and all digital data that can establish that a violation of the Executive Branch of NJ Information Security Policies and Standards has been committed or can provide a link between the violation of these policies and its victim or perpetrator.

Hardware: all of the physical components of a computer.

Information: refers to the data and programs that are stored or transmitted using a computer.

Bit-Stream Copy: a process whereby all data from a media device is duplicated, including slack space and unallocated space.

Message Digest Algorithm (MD5): The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

Secure Hash Algorithm (SHA-2): This is also referred to as the Secure Hash Standard (SHS). Like MD5, SHA-2 produces a unique message digest given a stream of bits.

11.6 United States Department of Justice Computer Crime Categories

Computer Crime Categories as defined according to the US Federal Guidelines for Searching and Seizing Computers. The categories are not mutually exclusive. Individual crimes can fall into multiple categories. These categories provide a framework for identifying what constitutes evidence and what needs to be searched and seized.

Hardware: Computer as contraband or fruits of the crime
Computer as an instrumentality
Computer as evidence

Information: Information as contraband or fruits of the crime
Information as an instrumentality
Information as evidence

11.7 Evidence Collection Methodologies

Collection Method	Crime Category	Advantages	Disadvantages
Collect Hardware	Hardware as fruit of crime Hardware as instrumentality Hardware as evidence Hardware contains a large amount of digital evidence	Requires little technical expertise Method is relatively simple and less open to criticism Hardware can be examined later in a controlled environment	Risk damaging equipment or not being able to operate it later Risk liability for unnecessary disruption of business Develop bad reputation for heavy handedness

Collect all digital evidence. Leave hardware	Information as fruits of the crime Information as instrumentality Information as evidence	Digital evidence can be examined later in a controlled environment Working with a copy prevents damage to original evidence Avoids liabilities of collecting hardware	Requires equipment and technical expertise Risk not being able to restart computer or accessing all evidence Risk missing evidence Time consuming Methods open to criticism
Only collect digital evidence that you need	Information as fruits of the crime Information as instrumentality Information as evidence	Allows for a range of expertise Can ask for help from system administrator or owner Practical, quick and inexpensive Avoid risks and liabilities of collecting hardware or evidence not specified in warrant	Can miss or destroy evidence
Source: Digital Evidence and Computer Crime: Forensic Science Computers and the Internet, Eoghan Casey, 1999			

References

Casey. Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego: Academic Press, 2000.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed. Berkeley, California: Osborne/ McGraw Hill, 1999.

Rosenblatt, Kenneth S. High Technology Crime: Investigating Cases Involving Computers. San Jose, California: KSK Publications, 1996.

U.S. Department of Justice, Computer Crime and Intellectual Property Section. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, D.C.: U.S. Department of Justice, Computer Crime and Intellectual Property Section, 2001

Mandia, Kevin and Chris Prosise, Incident Response, Investigating Computer Crime. Berkeley, California:

Osborne/McGraw Hill, 2001.

12 APPENDIX D: CIRT AND KEY CONTACTS LIST

Below is an Appendix list of OIT Cybersecurity Incident Response Team (CIRT), along with Key IT, Internal and External Contacts. Based upon the nature of the incident, these CIRT contacts may be called upon to respond to OIT's efforts to plan and mitigate cybersecurity incidents. Additionally, these members may call upon appropriate agency resources to support such efforts.

12.1 INTERNAL CONTACTS

OIT Cybersecurity Incident Response Team (CIRT)				
Name	Email	Work Phone	Cell Phone	Title
Allison J Davis	allison.davis@tech.nj.gov	609-376-7537	609-358-1677 267-467-0261	OIT CISO/Director, Infrastructure Security
Kevin Dehmer	Kevin.Dehmer@tech.nj.gov	609-376-8000	609-376-8000	Chief Technology Officer
Laura Console	Laura.Console@tech.nj.gov	609-649-0445	609-649-0445	Chief of Staff
Vernon Spencer	Vernon.Spencer@tech.nj.gov	609-826-3617	609-422-7093	Chief Operating Officer
Joseph Barber	Joseph.Barber@tech.nj.gov	609-300-2328	609-571-0364 609-731-0922	Deputy CTO Network Operations
Hagen Hottmann	Hagen.Hottmann@tech.nj.gov	609-376-7099	609-273-2513	Deputy CTO, Enterprise Services
Mandrele Hansford	Mandrele.Hansford@tech.nj.gov	609-826-3667	609-414-4277	Deputy CTO, Applications & Customer Service
Joseph Roe	Joseph.Roe@tech.nj.gov	609-826-3641	609-633-6465	Deputy CTO, NJOIT Managed Hosting Services and Mainframe Operations
Yolanda Windom	Yolanda.Windom@tech.nj.gov	609-826-3630	609-331-2734	Director, Data Center, Facilities & Disaster Recovery
John Seith	John.Seith@tech.nj.gov	609-826-3643	609-306-9879	Manager, Cloud Operations, Enterprise Public Cloud
Julie Garland Veffer	Julie.Veffer@tech.nj.gov	609-815-2140	609-947-7040	Director, Communications and Digital Services
Poonam Soans	Poonam.Soans@tech.nj.gov	609-376-7259	609-203-9934	Chief Data Officer & Director of Application Development

OIT Key Contacts				
Name	Email	Work Phone	Cell Phone	Title
Ashit Vyas	ashit.vyas@tech.nj.gov	609-376-7107	609-915-2358	Manager/ Enterprise Change, Asset & Configuration Management
Rupal Bhandari	Rupal.Bhandari@tech.nj.gov	609-940-1133		Supervisor, Incident & Solution Mangement
Brian Gadsby	Brian.Gadsby@tech.nj.gov	609-403-7009	609-508-3780	Manager, Data Center Services
Kevin Julius	Kevin.Julius@tech.nj.gov	609-376-7044	609-475-2420	Asst. Director, Network Services
Victor Staniec	Victor.Staniec@tech.nj.gov	609-954-4460	609-954-4460	Manager, Network Services

Denise Reed	Denise.Reed@tech.nj.gov	609-422-7183	609-672-4068	Supervisor, Infrastructure Security
Jay Hoffacker	Jay.Hoffacker@tech.nj.gov	609-875-4671		Supervisor IT, Infrastructure Security, Privilege Access
Sandra Stevens	Sandra.Stevens@tech.nj.gov	609-376-7048	609-341-6474	Network Admin 2, Extranet and Firewall Access
Michael Morgan	Michael.Morgan@tech.nj.gov	609-376-7162	609-610-0674	Director, Office of Emergency Telecommunications Services
B. Wayne Higgins Jr	barry.higgins@tech.nj.gov	609-376-7239	609-960-3894	Asst. Director/Managed Hosting Windows, VMware, Capacity Planning
Jeffrey Miglin	jeffrey.miglin@tech.nj.gov	609-376-7554	609-433-2673	Supervisor/Linux, Solaris, AIX
Melissa Mercado	Melissa.Mercado@tech.nj.gov	609-826-3644	609-433-2196	Network Admin. 2, Storage, Managed Hosting & Mainframe Services
Thomas DeHaan	Thomas.DeHaan@tech.nj.gov	609-815-2033	609-273-9048	Supervisor, Service Level Management
Elliott Lynn	Elliott.Lynn@tech.nj.gov	609-376-7541		O365 & Entra ID Services
Sandra Gambino	Sandra.Gambino@tech.nj.gov	609-376-7090	609-508-6675	Director, Mainframe Services
Bernadette Rainey	Bernadette.Rainey@tech.nj.gov	609-376-7190	*609-649-0900*	Supervisor, Mainframe Services
Leslie Rodenberger	Leslie.Rodenberger@tech.nj.gov	609-376-7089	*609*-775-5549	Supervisor, Mainframe Services
Karen Krenzel	Karen.Krenzel@tech.nj.gov	609-376-7126	609-433-5602	DR/COOP Team Lead

OIT Key Legal/HR Contacts				
Name	Email	Work Phone	Cell Phone	Title
Brandon Bowers	Brandon.Bowers@tech.nj.gov	609-376-7164	609-940-9926	Director, Legal/Compliance/Privacy
Heather Pursell	heather.pursell@tech.nj.gov	609-376-7065	(609) 649-1687	Manager, Human Resources

12.2 EXTERNAL CONTACTS

Key External Contacts				
Name	Email	Work Phone	Cell Phone	Title
Roza Dabaghyan	Roza.Dabaghyan@law.njoag.gov	609-376-3157		OIT NJ Attorney General Rep
Michael T. Geraghty	mgeraghty@cyber.nj.gov	609-815-5068	571-236-2642	State of NJ – Chief Information Security Officer, NJ Cybersecurity & Communications Integration Cell
Robert Bruder	RBruder@cyber.nj.gov	609-256-4831	609-433-9034	State of NJ– Deputy Chief Information Security Officer, NJ Cybersecurity and Communications Integration Cell
Michael Dunn	Michael.Dunn@treas.nj.gov	609-826-3536		DPP/Cyber Insurance Point of Contact

13 STATE OF NEW JERSEY CYBERSECURITY INCIDENT RESPONSE PLAN VERSION HISTORY

Revision #	Date	Changes Made	Made By
1.0	06/23/2025	Plan Draft	Allison J. Davis
1.1	07/22/2025	Updated Contact Details in Appendix D	Allison J. Davis
2.0	05/01/2026	Plan Draft	Allison J. Davis
2.1	05/19/2026	Updated Contact Details in Section 6.1 and Appendix D	Allison J. Davis