NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 191- Information Security Incident Management Response Procedure	**POLICY NO:** 11-02-P2-NJOIT	
	SUPERSEDES: 11-03-P1-NJOIT	**EFFECTIVE DATE:** 05/24/2012
	VERSION: 3.0	**LAST REVIEWED:** 07/24/2013

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this procedure is to establish response protocols for security incidents in the Executive Branch of New Jersey State Government's computers, systems, and infrastructure. This document provides procedures to support the implementation of the Office of Information Technology Policy 11-02-NJOIT (190 – Information Security Incident Management Policy).

Note: This procedure deals with cyber (information technology) security and does not address the physical security of facilities or assets. Response to a physical security breach will be governed by the appropriate policies/procedures. If unauthorized physical access to a technology resource leads to unauthorized logical access to State information, multiple reporting policies, including this policy, apply.

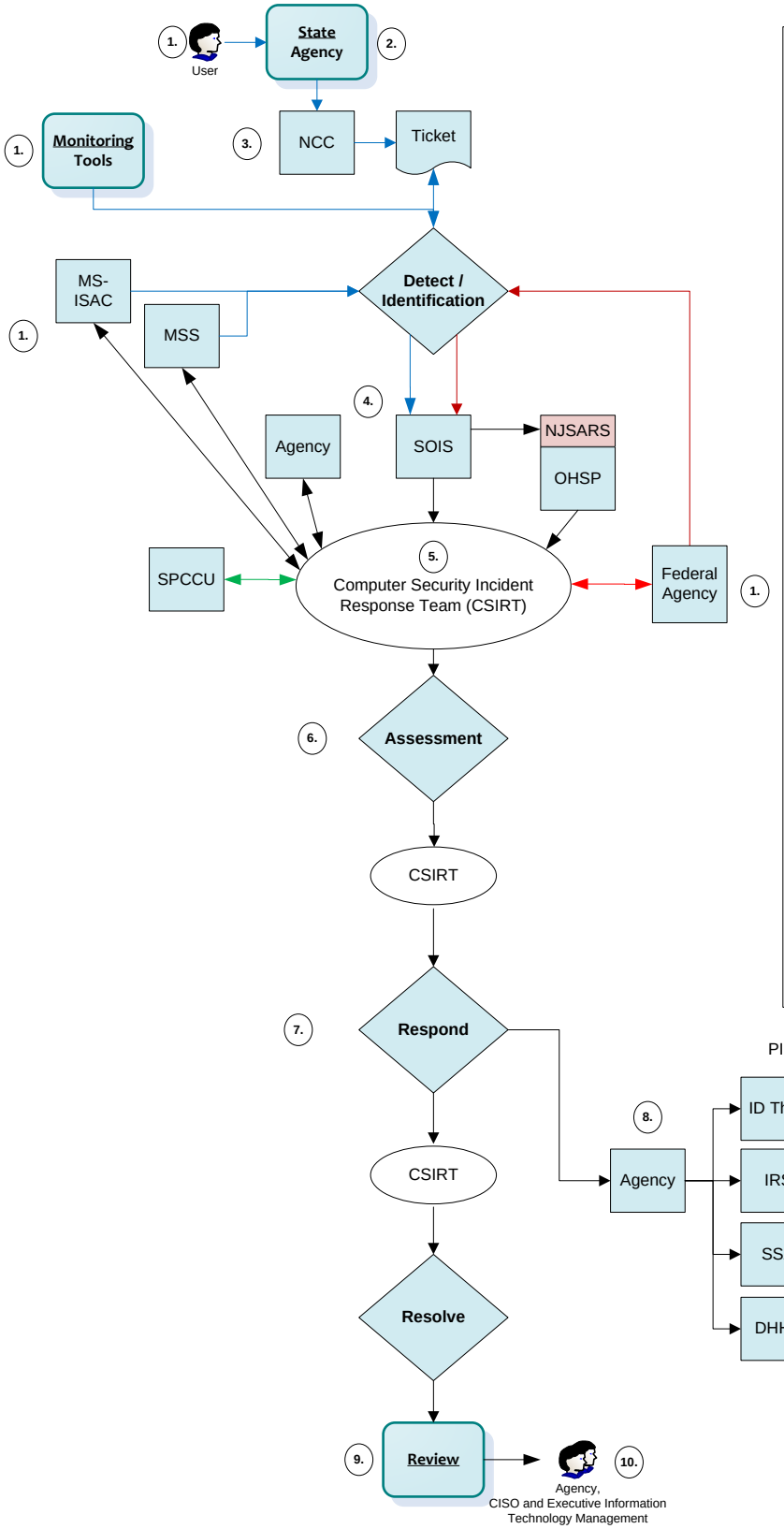
2 AUTHORITY

This procedure is issued under the authority of NJOIT Policy 11-02-NJOIT, (190 – Information Security Incident Management Policy).

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular to comply with changes in NJOIT or other agency policies.

3 SCOPE

This procedure applies to all personnel, including employees, temporary workers, volunteers, contractors and those employed by contracted entities, and others tasked with the execution of the Incident Management Response Policy.



1. Report of suspicious event or incident.

2. A representative from the Agency's IT organization will fill out the Incident Reporting form.

3. NCC personnel shall receive and record all event and/or incident, direct that ticket to the SOIS.

4. SOIS confirms the reported information on suspected incident and identifies response actions, and assigns an appropriate severity level. A severity level 5, 4 or 3 will be reported to NJSARS for the appropriate notifications.

5. SOIS establishes a response team (CSIRT).

6. Response team collect data in support of the incident.

7. Response team provide general containment actions.

8. The agency reports the incident to the appropriate authorities.

9. SOIS and departments and/or agencies meet to review incident that involves a criminal investigation or information security breach.

10. The final report is given to the agency, CISO and Executive Information Technology Management.

4 PROCEDURES

No single unit within NJOIT or other agencies are chartered or staffed to fully investigate, contain, or resolve information security incidents. The information security incident response process relies on all units within NJOIT and other agencies for successful resolution of information security incidents.

The procedure provides a coordinated approach in identification, assessment, response, and review.

5 INCIDENT CONFIRMATION (IDENTIFICATION)

Upon receipt of a suspected information security incident report per 11-02-P1- NJOIT 190-00-01 Incident Management Response Procedures, the Statewide Office of Information Security (SOIS) will confirm the reported information to determine the scope of the suspected incident and response actions.

The SOIS will assign an appropriate severity level to the confirmed incident and determine any subsequent response actions.

Incidents shall be grouped into five (5) different severity levels with broad sets of criteria for each level, based on the severity level requirements. For example:

5.1 Severity 1 Low

The severity and MS-ISAC alert level indicates credible warnings of increased probes or scans detected on systems; infected by known low risk malware; intelligence received concerning threats to which systems may be vulnerable; normal activity with low level of impact.

In certain instances severity 1 security incidents maybe viewed informational in nature and will be handled via routine day to day procedures. If a determination is made that the event is not adverse, then the event / incident ticket will be closed.

5.2 Severity 2 Guarded

The severity and MS-ISAC alert level indicates a change in normal activity with minor level impact; a vulnerability is being exploited with minor impact; infected by malware with the potential to spread quickly; compromise of non-critical system(s) that did not result in loss of sensitive data; a distributed denial of service attack with minor impact.

5.3 Severity 3 Elevated

The severity and MS-ISAC alert level indicates a significant risk due to an exploit for a vulnerability that has a moderate level of damage or disruption; compromise of secure or critical system(s); compromise of system(s) containing sensitive information or non-information; more than one entity (agency) affected in the network with a moderate level of impact; infected by malware that is spreading quickly throughout the Internet with moderate impact; a distributed denial of service attack with moderate impact.

5.4 Severity 4 High

The severity and MS-ISAC alert level indicates a high risk of malicious activity impacting core infrastructure; a vulnerability is being exploited and there has been major impact; data exposed with major impact; multiple system compromises or compromises of critical infrastructure; attackers have gained administrative privileges on compromised systems; multiple damaging or disruptive malware infections; mission critical application failures but no imminent impact on the health, safety or economic security of the State; a distributed denial of service attack with major impact.

5.5 Severity 5 Severe

The severity and MS-ISAC alert level indicates a severe risk due to malicious activity resulting in widespread outages and/or complete network failures; data exposure with severe impact; significantly destructive compromises to systems, or disruptive activity with no known remedy; mission-critical application failures with imminent impact on the health, safety or economic security of the State; compromise or loss of administrative controls of critical systems; loss of critical supervisory control and data acquisition (SCADA) systems.

The SOIS shall maintain continuous updates of the event / incident ticket.

Incident response times are contingent on several factors, such as the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing Service Level Agreements (SLA) for affected resources, the time and day during the week, and other incidents that the team is handling. Generally, the highest priority is handling incidents that are likely to cause the most damaged to the organization or can affect multiple organizations.

Any communications and internal notification processes will be coordinated through the SOIS. In certain instances, communications will be handled through the Agency's Public Information Officer.

5.5.1 Severity 2, 3, 4, or 5 Escalation

The Chief Information Security Officer (CISO) or designee will brief the State's Chief Information Officer (CIO) throughout the life cycle of the incident.

The CISO or designee will notify the State of New Jersey's Office of Homeland Security and Preparedness (OHSP) of the incident by entering the incident report into the New Jersey's Suspicious Activity Reporting System (NJSARS). Dissemination of Cyber Incident SARS incidents will be to the Cyber Incident Notification Group which is managed by NJOIT and OHSP.

The CISO or designee will notify the Multi-State Information Sharing and Analysis Center (MS-ISAC) of the incident. MS-ISAC will coordinate with the Federal government and provide assistance with remediation strategies if requested by the State of New Jersey.

5.5.2 Criminal activity

In the event that criminal activity is suspected or confirmed, the incident will be handled by the CISO or designee on behalf of the impacted Department and/or Agency, and shall request assistance from the Federal Bureau of Investigation and/or New Jersey State Police Cyber Crimes Unit.

The events will proceed as follows:

5.5.2.1 Federal Bureau of Investigation and/or the State Police Cyber Crime Unit will be contacted.

5.5.2.2 A basic determination on intent will be made by the FBI and/or State Police Cyber Crime Unit.

5.5.2.3 Federal Bureau of Investigation and/or State Police Cyber Crime Unit will meet the liaison at the location if the event is deemed criminal and investigate the situation.

5.5.2.4 If needed, the Federal Bureau of Investigation and/ or State Police Cyber Crime Unit will remove any computer or equipment for analysis.

5.5.2.5 If any other law enforcement agency's participation is required, the State Police Cyber Crime Unit will be the direct contact to that agency.

5.5.2.6 Any incident not deemed criminal in nature shall be directed back to CISO for action.

6 INCIDENT INVESTIGATION (ASSESSMENT) AND CONTAINMENT (RESPOND)

In the Investigation and Containment phase, actions will be taken to contain the damage through the coordinated effort of various incident responders. Depending on the incident type and/or severity level, a response team may be assembled to investigate, contain, and resolve the incident. The SOIS will administer the coordination of investigation and containment activities, including establishing a Computer Incident Response Team (CSIRT).

6.1 The CSIRT's personnel shall collect data in support of the incident by investigating sources such as host and application data, networks and network devices, intrusion detection sensors and agents with all data being collected in a timely manner.

The integrity of the collected data must remain intact throughout the life cycle of the investigation.

6.2 The CSIRT's personnel shall provide the general containment actions where practicable or applicable and may involve shutting down systems, temporarily disabling system/network services, increasing monitoring of system and network activities, turning on auditing capabilities, examining system logs, and verifying that redundant systems have not been compromised.

6.3 If it is determined that it is necessary to isolate an offending system from the Garden State Network as a result of an incident the following procedures will be initiated by the responding personnel lead:

6.3.1 Notify the department and/or agency of pending termination

6.3.2 Terminate Garden State Network connectivity

6.3.3 Assist with remediation as applicable

6.3.4 Verify remediation

6.3.5 Reconnect Garden State Network connectivity

6.3.6 The CIO and appropriate Agency Executives to be briefed on such incidents

After review of the incident discovered during the investigation, the CSIRT's personnel will make recommendations to the Agency. Agencies must take the necessary next step to remediate the incident.

Note: All incidents will be tracked through the NCC with the SOIS updating ticket information as needed.

6.4 Gathering and Collecting "Evidence"

During incidents that receive a criminal investigative response, the Federal Bureau of Investigation and/or State Police Cyber Crime Unit will gather and collect all evidence that may be required for remediation or administrative inquiry. This evidence will be duplicated in a forensically sound manner as determined by law enforcement prior to removal from the scene. Duplicates will be retained by the team responsible for remediation. Original evidence will become inaccessible after seizure.

7 INCIDENT RESOLUTION (RESOLVE)

An incident is considered resolved when all affected systems and services are restored to a state that provides necessary services, but is no longer vulnerable.

If systems that may have thought to be restored continue to show incidents, that system shall be isolated from the State's infrastructure until the problem has been remediated.

The SOIS will compile and store the collected data, and close the incident ticket when the incident is resolved.

7.1 Incident REPORT

7.1.1 Severity 2, 3, 4, or 5 escalation

The CISO or designee will brief the CIO of the incident resolution if the severity level is a 2, 3, 4 or 5.

CISO or designee will notify OHSP of the incident resolution by entering the incident report and updates into the New Jersey's Suspicious Activity Reporting System (NJSARS).

The CISO or designee will notify the Multi-State Information Sharing and Analysis Center (MS-ISAC) of the incident resolution.

If the incident consisted of an information security breach, containing personally identifiable information (PII), the agency is also to follow the Division of Consumer Affairs' policy:

(http://www.njconsumeraffairs.gov/adoption/dcado47.htm)

If the PII security breach consisted of social security numbers, the agency is to follow the IRS Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies (http://www.irs.gov/pub/irs-pdf/p1075.pdf) and Section 10, Reporting Improper Inspections or Disclosures and the Information Exchange Agreement between the SSA and the State of New Jersey: (http://www.irs.gov/pub/irs-pdf/p1075.pdf).

If the PII security breach consisted of health information, the agency is to follow the Federal requirements Department of Health and Human Services, 45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information; Interim Final Rule (http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf).

8 INCIDENT FOLLOW-UP (REVIEW)

Depending on the severity level and the impact of the incident, a follow-up meeting maybe required. The CISO will coordinate a meeting with the CSIRT to review the response and remediation process.

SOIS and NJOIT shall monitor corrective measures for issues or unseen side effects as well as determine whether more problems were introduced, than solved.

SOIS will coordinate a follow-up meeting with departments and/or agencies for any incident that involves a criminal investigation or information security breach.

9 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this procedure within 90 days of its effective date.

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and noncompliance with this policy will be managed in accordance with Policy 08-02-NJOIT (111 – Information Security Managing Exceptions).