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 190-NJOIT - Information Security Incident Management Policy	**POLICY NO:** 11-02-NJOIT	
	SUPERSEDES: 11-03-NJOIT	**EFFECTIVE DATE:** 05/24/2012
	VERSION: 2.0	**LAST REVIEWED:** 05/24/2012

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

This policy establishes the authority of the New Jersey Office of Information Technology (NJOIT) to oversee the management of information incidents across the Executive Branch of New Jersey State Government. This policy also establishes the responsibility for reporting and responding to events and/or all suspected information security incidents observed on the Executive Branch of New Jersey State Government's computers, systems, and infrastructure.

NOTE: This policy deals with cyber information security and does not address the physical security of facilities or assets. Response to a breach in physical security will be governed by the appropriate policies. If unauthorized physical access to an information resource leads to unauthorized cyber related access to state information, multiple reporting policies, including this policy shall apply.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey P.L.2007.c.56. This order defines NJOIT's role with regard to technology within the community of the Executive Branch of State Government.

NJOIT reserves the right to change or amend this circular.

3 SCOPE

This policy applies to all personnel including employees, temporary workers, volunteers, contractors, those employed by contracted entities and others authorized to access enterprise assets and information resources.

4 DEFINITIONS

Please refer to the Statewide Policy Glossary at http://www.nj.gov/it/ps/glossary/.

5 POLICY

5.1 Incident Reporting

The Statewide Office of Information Security (SOIS) will ensure that a viable Incident Management Reporting process is in place that will enable personnel to promptly report all suspicious cyber related information security events and/or incidents. The SOIS will execute central authority and responsibility oversight for recording and responding to Information Security incidents as part of its Information Security Incident Management Program.

All Executive Branch Departments and Agencies within the New Jersey State Government shall adopt and implement these Incident Management Reporting policies and procedures, in addition to any individual Departmental and/or Agency reporting requirements.

Department or Agency Incident Management Reporting policies shall not conflict with, or supersede established enterprise policies.

5.1.1 All personnel within all Departments and Agencies shall report all suspicious cyber related information security events and/or incidents that have the potential to expand beyond the local systems, networks, and/or network infrastructure to the Network Call Center (NCC) (800-622-4357) according to the procedures outlined in *11-02-P1-NJOIT - 190-00-01 Information Security Incident Management Reporting Procedure*. All personnel are required to report "events or incidents" even if they have contributed in some way to the event or incident.

Note: Examples of incidents are included in 11-02-P1-NJOIT - 190-00-01 Information Security Incident Management Reporting Procedures attachment A to assist with the understanding of incident reporting terms, concepts, and requirements presented in this policy. These examples are illustrative in nature and do not represent all possible events or incidents that may occur.

5.1.2 Departments and Agencies are to handle internal suspicious cyber related information security events and/or incidents that occur on their Department/Agency's computers and systems, although if an event occurs which impacts multiple computers or systems, the local area network or a facility it should be reported to NJOIT.

5.1.3 All Department and Agencies shall report any suspected criminal action to the Chief Information Security Officer (CISO), who will contact the appropriate law enforcement and/or investigative authorities.

Any attempt to interfere with, prevent, obstruct, or dissuade anyone in his or her efforts to report a suspicious cyber information security incident is prohibited.

Any form of retaliation against an individual reporting or investigating information security incidents is prohibited.

The CISO and/or SOIS personnel shall determine whether an event is an incident and the degree to which information and/or information resources have been compromised.

All reported security events and/or incidents shall be promptly investigated and documented according to the Information Security Incident Management Reporting policy and procedure. If appropriate, a reported incident and/or event will be assessed to determine whether further action is required or remediation is necessary.

All documents associated with the response to information security incidents and/or violations shall be retained for a period of 3 years after the security incident has been investigated and determined closed by the CISO. Retention of all records stored electronically is subject to the Division of Archives and Records Managements (DARM) retention and destruction of records rules. Where a law or other regulation may require records to be maintained longer or if there were a litigation hold or a reasonable anticipation of litigation relating to a particular issue, the extended time frame would take precedence.

5.2 Incident Response

The New Jersey Office of Information Technology (NJOIT) Statewide Office of Information Security (SOIS) will serve as the central authority to ensure a consistent and effective process is in place for a coordinated approach to Information Security incident response by establishing an incident response team. The process will provide information sharing, containment, remediation, resolution of events, follow-up analysis, and documentation including any follow-up lessons learned.

The Chief Information Security Officer (CISO) and/or responding personnel will determine whether any event in question qualifies as a security incident and establish the severity level of the incident and will provide an appropriate response.

Routine detection and remediation of a virus, malware, or similar issue that has little effect on the day-to-day business and does not have the potential to expand beyond the local network is not considered an incident under this policy.

Incident response information is confidential and should only be distributed on a need to know basis. SOIS shall ensure that information and sharing analysis along with event correlation information is appropriately disseminated to government entities and law enforcement organizations.

All personnel within all Departments and Agencies shall cooperate with the NJOIT, Federal agencies, and any law enforcement agencies in the investigation of and response to information security events and/or incidents.

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 Personal Identifiable Information (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.

6 RESPONSIBILITIES

6.1 Departments and Agencies

All Departments and Agencies are required to adhere to the Incident Management policy and to report security incidents according to the procedures outlined in 190-00-01 Information Security Incident Management Response and/or Reporting procedures.

6.2 Chief Information Security Officer (CISO) and the Statewide Office of Information Security (SOIS)

The CISO and SOIS are responsible for oversight of this policy, and incident management assistance as required, to address the information security incidents.

6.3 Network Call Center Personnel (NCC)

NCC personnel shall receive and record all Event/Incident reports, and track the status of Event/Incident reports according to the incident reporting procedures.

6.4 Public Information Officer

The Department or Agency's Public Information Officer shall be responsible for handling all media and any public request for information.

6.5 Office of Homeland Security and Preparedness (OHSP)

OHSP is responsible for maintaining and operating the New Jersey's Suspicious Activity Reporting System (NJSARS). The Cyber Incident SAR will be processed and disseminated by the OHSP Counter Terrorism Watch (CTWatch). NJOIT and OHSP will manage the Cyber Incident Notification Group list.

6.6 Multi-State Information Sharing and Analysis Center (MS-ISAC)

MS-ISAC is responsible for coordinating with the Federal government on behalf of the State of New Jersey and will provide assistance with information sharing, early warnings and alerts, mitigation strategies, training, and exercises and for maintenance of overall cyber situational awareness.

6.7 Federal Bureau of Investigation and the New Jersey State Police Cyber Crimes Unit

The Federal Bureau of Investigation and NJSP Cyber Crimes Unit shall be the final determinant as to what criminal investigative resources will be directed at a given incident.

Copies of Incident Management Response and/or Reporting Procedures will be distributed by request only.

7 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy 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*).