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 190-00-01 Information Security Incident Management Reporting Procedure	**POLICY NO:** 11-02-P1-NJOIT	
	SUPERSEDES: 11-03-P1-NJOIT	**EFFECTIVE DATE:** 05/24/2012
	VERSION: 3.0	**LAST REVIEWED:** 07/26/2013

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this procedure is to establish enterprise reporting protocols for suspicious cyber related information security incidents and/or events for the Executive Branch of New Jersey State Government's computers, systems, and infrastructure.

2 AUTHORITY

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

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

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

4 PROCEDURE

The Office of Information Technology's Statewide Office of Information Security (SOIS) shall oversee the incident reporting process and shall maintain communications within NJOIT and other Departments and Agencies. The SOIS shall maintain records of Departmental and Agency Points of Contact (POCs) in support of incident reporting.

The Chief Information Security Officer (CISO) or designee shall ensure that incident reporting procedures are documented and all personnel are informed of their responsibilities.

4.1 DETECTION AND REPORTING

All Departmental and Agency personnel shall report all suspicious information security events or incidents that have the potential to expand beyond the local network promptly to the NJOIT Network Call Center (NCC) by calling **800-NCC-HELP** (800-622-4357). This is in addition to any internal Departmental or Agency reporting processes that may be in place.

4.1.1 Departments and Agencies will use Attachment (A) and Incident Reporting Form as an initial step in gathering and reporting information to the NCC.

4.1.2 NCC personnel shall receive and record all events to establish a ticket and direct that ticket to the SOIS. The reporting Department/Agency will be given the ticket number to reference.

4.1.3 The SOIS will coordinate and distribute the ticket to any additional assignment group(s) as appropriate.

4.1.4 The CISO or designee will notify OHSP of the incident if the severity of the incident affects a significant numbers of computers, systems or a critical infrastructure; isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus; isolated integrity and/or availability breaches; widespread instances of known computer viruses easily handled by anti-virus software. Reference the State of New Jersey IT Circular 191-00-01 Information Security Incident Management Response Procedure and severity level is a 2, 3, 4 and 5.

4.1.5 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. Reference the State of New Jersey IT Circular 191-00-01 Information Security Incident Management Response Procedure and severity level is a 2, 3, 4 and 5.

4.1.6 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.

4.1.7 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.

4.1.8 During normal business hours, the State Police Cyber Crimes Unit can be reached at 609-584-5000 x5664. Outside of normal business hours, the Cyber Crimes Unit can be reached via the NJ Regional Operations and Intelligence Center at 609-963-6951.

4.1.9 All reported incidents shall be reviewed by the CISO or designee along with any other assignment group(s).

All reported security events and/or incidents shall be promptly investigated and documented. The CISO and/or responding personnel shall determine whether an event is an incident and the degree to which information and/or information resources have been compromised. If appropriate, a reported event and/or incident will be assessed to determine whether further action is required or remediation is necessary. The reporting Agency/Department should be informed in writing of the CISO disposition of the incident.

All documentation associated with reported information security events and incidents will be retained for a period of 3 years or the life cycle of the incident or whichever is longer.

5 WHAT USERS SHOULD DO WHEN EXPERIENCING AN EVENT OR INCIDENT

5.1 Contact the NCC and report the event and/or incident.

5.2 Do not attempt:

5.2.1 To prove that a system or network has a weakness. Only authorized personnel are permitted to employ vulnerability-scanning tools against enterprise networks, assets, or resources.

5.2.2 To remediate or attempt any computer forensic work.

5.2.3 To discuss suspicious cyber incidents with anyone beyond what is required to report the incident to the NCC and/or your reported chain of command. Refer all media or public requests for information related to Incidents or suspected incidents to your Department or Agency Public Information Officer.

6 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 procedure because of business reasons or system constraints. Exceptions and non-compliance with this procedure shall be managed in accordance with Policy 08-02-NJOIT (111 – Information Security Managing Exceptions).