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**<br>161 –Operational Security Policy | **POLICY NO:**<br>**14-05-NJOIT** | |
| | **SUPERSEDES:**<br>NEW | **EFFECTIVE DATE:**<br>01/07/2014 |
| | **VERSION:**<br>1.0 | **LAST REVIEWED:**<br>01/07/2014 |

ATTN: Directors of Administration and Agency IT Directors

# 1 Purpose

The purpose of the policy is to provide for the proper protection of the State of New Jersey operations by identifying the potentially vulnerable areas within operational processes that contain the greatest risk to the State's operational security.

This policy addresses an operational security program that needs to be observed in order to protect the State of New Jersey's systems.

# 2 Authority

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

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

# 3 Scope

This policy applies to all personnel, including employees, temporary workers, volunteers, contractors, and those employed by contracting entities, and others who are tasked with the protection of the State of New Jersey information and property through the use of operational security controls.

# 4 DEFINITIONS

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

# 5 POLICY

This policy establishes operational security responsibilities. Agencies and their system owners are responsible to ensure security control standards and procedures are followed in accordance with State and Federal security requirements.

This policy is based on the assumption that agencies have or will establish operational security controls and procedures that protect the State's information and equipment from confidentiality, integrity, and availability vulnerabilities.

## 5.1 Awareness Training

5.1.1 All state employees shall complete security awareness training annually and be exposed to security awareness materials throughout the year as provided in (*12-01-NJOIT, 141 – Security Awareness Program Policy*).

5.1.2 Users shall receive additional specialized security training as required by changes in the technologies, their security responsibilities or State and Federal regulations.

## 5.2 Configuration Management

5.2.1 Agencies shall establish configuration baselines for their systems and restrict who has access to make changes to those baselines.

5.2.2 Agencies shall establish a Change Control Workgroup (CCW) that will meet regularly to review change requests.

5.2.3 CCW members shall be chosen to ensure that requested changes are thoroughly checked and assessed from a security, technical and business perspective.

5.2.4 The use of functions, ports, protocols, and services not required to perform essential capabilities on systems for receiving, processing, storing, or transmitting confidential information, shall be disabled.

## 5.3 Contingency Operations

**5.3.1** Backup operations

5.3.1.1 *Backup of IT System resources must be done regularly by support and operation's personnel.*

5.3.1.2 *Backup of local media on computer systems (PCs) are the responsibility of the user.*

5.3.1.3 *Frequency of backups will depend on regulatory requirements, or upon how often data changes and how important those changes are to agency operations.*

5.3.1.4 *Backup procedures must be periodically tested to ensure that they can be used to copy work as intended and can be relied upon for emergency use when necessary.*

5.3.1.5 *Backups will be stored securely and moved offsite when possible.*

**5.3.2** All systems will have a contingency plan. The plan's purposes will be to decrease the risks of business interruptions and minimize the impacts of service disruptions. The plan will be executed at the direction of the system owner when an emergency occurs at the primary processing site.

5.3.3 All agencies should have an alternate processing site should the primary data center site become unavailable.

## 5.4 Incident Response

Each agency must follow the policy *11-02-NJOIT, 190 – Information Security Incident Management Policy* and implement procedures as per *11-02-P1-NJOIT, 190-00-01 Information Security Incident Management Reporting Procedure* to include the following:

5.4.1 Security Incident Criteria – The Statewide Information Security Officer (SISO) and/or responding personnel shall determine whether an event is an official security incident that requires further investigation and action. They also will determine the degree to which information and/or information resources may have been compromised.

5.4.2 Report – All agencies are required to record and report an incident to the proper authorities if its severity or criminality so warrant.

5.4.3 Response – The Statewide Office of Information Security shall take steps to end weaknesses that were exploited and services.

5.4.4 Notification Process – The Statewide Office of Information Security shall ensure that information and sharing analysis along with event correlation information is appropriately disseminated to government entities and law enforcement organizations.

## 5.5 System Maintenance

5.5.1 Records of all maintenance performed on State of New Jersey information systems should be maintained for at least one year.

5.5.2 All vendor maintenance tools should be approved by the system owner for the protection of the system being maintained.

5.5.3 Remote maintenance by vendors should be approved by the system owner before being permitted.

## 5.6 Media Protection

5.6.1 Agencies shall establish physical and logical controls and procedures that protect system media (paper or digital), from unauthorized access, modification, destruction or loss.

5.6.2 Agencies shall adhere to the policies set forth in the *09-10-NJOIT, 152 – Information Disposal and Media Sanitization.*

## 5.7 Physical Security

5.7.1 Appropriate control mechanisms or procedures shall be applied to alert and prevent unauthorized entry attempts into non-public facilities and offices. Access to areas within facilities that house sensitive or critical state information resources shall have additional controls that restrict and monitor access into these areas to authorized persons only.

5.7.2 Data centers shall be equipped with alarm systems that monitor, log, and automatically alert staff to anomalies relating to fire/smoke, water, temperature, humidity, chemical and electrical effects, and physical intrusion.

5.7.3 Continuity of power (e.g. UPS, backup generators) shall be provided to maintain the availability of critical production systems.

5.7.4 Physical entry into data centers shall have mechanisms or procedures that expressly restrict and monitor access to only authorized persons. All visitor access shall be with an escort.

5.7.5 Access into data centers shall be logged and maintained, containing names and entry/exit times.

5.7.6 Access lists/logs into data centers shall be reviewed and updated regularly.

## 5.8 Personnel Security

5.8.1 Agencies should verify the identity, employment eligibility and conduct background screenings, where applicable, for all State employees and engagement contractors before granting access credentials to State of New Jersey facilities or information resources not designated as public access resources.

5.8.2 Agencies should ensure that individuals occupying positions of responsibility within their organization (including third-party service providers) meet established security and qualification criteria for those positions.

5.8.3 Agencies should ensure that organizational information and information systems are protected during and after personnel actions such as terminations and/or transfers.

5.8.4 Agencies should employ formal sanctions for personnel failing to comply with security policies and procedures.

5.8.5 Any agency sponsoring a contract with a third party shall assess and manage the risks associated with granting any access or outsourcing any services to that third party or parties.

## 5.9 System Integrity

5.9.1 System Owners shall incorporate policy, education and awareness as well as technical controls to mitigate the risks of incidents from malicious code in state information systems.

5.9.2 Agencies shall adhere to the policies set forth in the *14-01-NJOIT, 171 – Minimum System Security and Protection Policy*.

5.9.3 All agencies should promptly (automatically, if possible) install security-relevant software updates such as patches, service packs, and hot fixes.

5.9.4 All agencies should perform monitoring of their Information Systems at strategic locations with tools such as Intrusion Detection Systems.

5.9.5 Where appropriate, agencies should employ integrity verification applications that scan the system for evidence of information tampering, errors, and omissions.

5.9.6 Agencies should provide for inspection of any electronic mail attachments and downloads for malicious software before use – this check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization. Spam protection should be provided on all electronic mail as well.

5.9.7 Agencies shall receive and review information system security alerts/advisories for critical software that they use (operating systems, applications, etc.) on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

# 6 EXCEPTIONS AND NON-COMPLIANCE

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

Failure to comply with this policy may result in disciplinary action. Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular *08-02-NJOIT, 111 – Information Security Managing Exceptions*.