NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Policy	**No:** NYS-P03-002
IT Policy: **Information Security**	**Updated:** 11/23/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for all State Entities (SEs) as defined below in Section 3.0 Scope. Any SE may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other Office of Information Technology Services' (ITS) security policies and associated standards. This policy defines the responsibility of all SEs to:

- protect and maintain the confidentiality, integrity, and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- ensure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits SEs by defining a framework that will ensure appropriate measures are in place to protect the confidentiality, integrity, and availability of New York State (NYS) information; and ensure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures, and practices, and know how to protect SE information.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This policy applies to all SEs, defined as "State Government" entities as defined in *Executive Order 117*[1], issued January 2002, or "State Agencies" as defined in *Section 101 of the State Technology Law* including their employees, and all third parties (e.g., local governments, consultants, vendors, and contractors), that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different policy, it must include the requirements set forth in this one.

This policy encompasses all systems, automated and manual, for which New York State has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. It addresses all information, regardless of the form or format, which is created or used in support of business activities of SEs.

4.0 Information Statement

4.1 Organizational Security

a. Information security requires both an information risk management function (including cyber-related risk management) and an information technology security function. Depending on the structure of the SE, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

recommended that these functions be performed by a high-level executive or a group that includes high level executives.

1. Each SE must designate an individual or group to be responsible for the risk management function. For the purposes of clarity and readability, this policy will refer to the individual, or group, so designated as the Cyber Risk Coordinator (CRC) (*see* Exhibit 1 for a more detailed description of the role). The CRC is responsible for ensuring that:

    i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed from the perspective of the SE as an enterprise regarding the overall strategic goals and objectives of the SE in carrying out its core missions and business functions; and

    ii. the management of information assets, information system-related security risks, and other cyber-security risks is consistent across the SE, reflects the risk tolerance of the SE, and is considered along with other types of risks to ensure mission/business success.

2. Each SE must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks. For SEs that receive IT services as a member of one of the portfolios within ITS, the information security function may be fulfilled by the Chief Information Security Office (CISO) and Security Services Teams.

b. Information security risk decisions must be made through consultation with both function areas described in **a.** above.

c. Although the technical information security function may be outsourced to third parties, each SE retains overall responsibility for the security of the information that it owns. The function of the CRC must be performed within the SE.

4.2 Functional Responsibilities

4.2.1 State Entity executive management is responsible for:

1. evaluating and accepting risk on behalf of the SE;

2. identifying SE information security responsibilities and goals and integrating them into relevant processes;

3. supporting the consistent implementation of information security policies and standards;

4. supporting security within the SE through clear direction and demonstrated commitment of appropriate resources;

5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;

6. implementing a process for determining information classification and categorization, based on industry recommended practices, State directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

8. determining who, within the SE, will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;

9. participating in the response to security incidents;

10. complying with applicable notification requirements in the event of a breach of private information;

11. adhering to specific legal and regulatory requirements related to information security;

12. communicating legal and regulatory requirements to the ISO/designated security representative; and

13. communicating the requirements of this policy and the associated standards, including the consequences of non-compliance, to the SE workforce and third parties, and addressing adherence in third party agreements.

4.2.2 The ISO/designated security representative is responsible for:

1. maintaining familiarity with SE business functions and requirements;

2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;

3. assessing SE compliance with information security policies and legal and regulatory information security requirements;

4. evaluating information security risks and assisting the SE in understanding its information security risks and how to appropriately manage those risks;

5. representing and ensuring security architecture considerations are addressed;

6. advising on security issues related to procurement of products and services;

7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

8. disseminating threat information to appropriate parties;

9. participating in the response to potential security incidents;

10. participating in the development of enterprise policies and standards for NYS that consider SE needs; and

11. promoting information security awareness.

4.2.3 IT management is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

2. providing resources needed to maintain a level of information security control consistent with this policy;

3. identifying and implementing all processes, policies, and controls relative to security requirements defined by the SE's business and this policy;

4. implementing the proper controls for information owned by the SE based on the SE's classification designations;

5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and

7. implementing business continuity and disaster recovery plans.

4.2.4 The State Entity workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted to SEs;

2. protecting State information and resources from unauthorized use or disclosure;

3. protecting personal, private, sensitive information (PPSI) from unauthorized use or disclosure;

4. abiding by ITS Policy, NYS-P14-001, Acceptable Use of Information Technology Resources; and

5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

4.2.5 The CISO is responsible for:

1. providing in-house expertise as information security consultants to the SEs as needed;
2. developing the State's information security program and strategy, including measures of effectiveness;
3. establishing and maintaining enterprise information security policy and standards;
4. assessing SE compliance with information security policies and standards;
5. advising on secure system engineering;
6. providing incident response coordination and expertise;
7. monitoring the State networks for anomalies;
8. monitoring external sources for indications of SE data breaches, defacements, etc.
9. maintaining ongoing contact with security groups/associations and relevant authorities;
10. providing timely notification of current threats and vulnerabilities; and
11. providing awareness materials and training resources.

Associated Standard: NYS-S10-001, Continuing Professional Education Requirements for ISOs/Designated Security Representatives Standard

4.3 Separation of Duties

a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

b. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails, and management supervision.

c. The audit and approval of information security controls must always remain independent and segregated from the implementation of said controls.

4.4 Information Risk Management

a. Any system or process that supports SE business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

b. Risk assessments are required for new projects, implementations of new technologies, any significant updates, or changes to the operating environment, or in response to the discovery of significant vulnerabilities. Risk assessments are

required regardless if the work is done by SE, vendor/contractor, or any other third party on behalf of the SE.

c. SEs are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

d. Risk assessments must include additional considerations when systems, services, or information will reside, or be accessed from, outside of the Contiguous United States (CONUS) to ensure compliance with relevant statutory, regulatory, and contractual requirements.

e. Risk assessment results, and the decisions made based on these results, must be documented.

Associated Standard: NYS-S14-001, Information Security Risk Management Standard; NYS-S13-001, Secure System Development Lifecycle (SSDLC) Standard

4.5 Information Classification and Handling

a. All information, which is created, acquired, or used in support of SE business activities, must only be used for its intended business purpose.

b. All information assets must have an information owner established within the SE's lines of business.

c. Information must be properly managed from its creation, through authorized use, to proper disposal.

d. All information assets must be reviewed and reclassified (if needed) on a recurring basis, with a frequency determined by the SE. Any changes to the individual data elements of an information asset requires an immediate review.

e. An information asset must be classified based on the highest level necessitated by its individual data elements.

f. If the SE is unable to determine the confidentiality classification of information then it must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

i. Each classification has an approved set of baseline controls designed to protect the data asset and is aligned with NIST 800-53B Control Baselines for Information

Systems and Organizations. These controls must be evaluated, tailored, and implemented to meet business requirements.

j. The SE must communicate the requirements for secure handling of information to its workforce.

k. A written or electronic inventory of all SE information assets must be maintained by the SE.

Associated Standards: NYS-S14-002, Information Classification Standard; NYS-S13-003, Sanitization/Secure Disposal Standard;

4.6 Information Sharing

a. SE content made available to the general public must be reviewed according to a process to be defined and approved by the SE. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

b. PPSI must not be made available without appropriate safeguards approved by the SE.

c. For non-public information to be released outside a SE or shared between SEs, a process must be established that, at a minimum:

   1. ensures that an information classification has been performed and documented for the information to be released or shared;

   2. documents the intended use of the information;

   3. identifies the responsibilities of each party for protecting the information;

   4. defines the process and minimum controls required to transmit, store, and use the information;

   5. records the measures that each party has in place to protect the information;

   6. defines a method for compliance measurement;

   7. provides a signoff procedure for each party to accept responsibilities,

   8. establishes a schedule and procedure for reviewing the controls; and

   9. identifies an end date for the use of the information (if applicable).

d. In addition to the requirements in Section 4.6.c, when information classified as having a High Confidentiality requirement is to be released or shared, the SEs must ensure that they:

   1. have a formal written agreement (e.g., Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU), etc.), which

contains the requirements for the handling of information, in place prior to sharing that information with any other SE or other third-party.

2. designate the level of management who can give written approval for:

    i. the transportation or storage of information outside of an approved storage facility and
    ii. the transmission of information outside the SE.

Associated Standards: NYS-S14-002, Information Classification Standard

4.7 IT Asset Management

a. All IT hardware and software assets must be assigned by the SE to a designated business unit or individual within the SE.

b. SEs are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Associated Standard: NYS-S14-008, Secure Configuration Standard

4.8 Personnel Security

a. The SE workforce must receive general information security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on SE specific information security procedures, if required, must be completed before access is provided to specific SE sensitive information not covered in the general information security training. All information security training must be reinforced at least annually and must be tracked by the SE.

b. A SE must require its workforce to abide by the ITS Policy, NYS-P14-001, Acceptable Use of Information Technology Resources, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

c. All job positions must be evaluated by the SE to determine whether they require access to sensitive information and/or sensitive information technology assets.

d. For those job positions requiring access to sensitive information and sensitive information technology assets, SEs must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation, or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports

from federal, state, and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the SE to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the State.

e. A process must be established within the SE to repeat or review suitability determinations periodically and upon change of job duties or position.

f. SEs are responsible for ensuring all State-issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: NYS-S14-013, Account Management/Access Control Standard

4.9 Information Security Incident Management

a. SEs must have an incident response plan, consistent with New York State standards, to effectively respond to information security incidents.

b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that information security concerns are not being appropriately addressed, they may confidentially contact the New York State Cyber Command Center directly.

c. The New York State Cyber Command Center must be notified of any information security incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

Associated Standard: NYS-S13-005, Cyber Incident Response Standard; See also: Cyber Incident Reporting Procedure

4.10 Physical and Environmental Security

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.

c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information media must be secured and concealed to the extent possible to prevent a compromise of confidentiality, integrity, or availability.

e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times. Any maintenance performed remotely must be virtually escorted.

f. For SE information that has a High Confidentiality requirement, written procedures must be created and implemented to keep track of individual documents, files, devices, or media and the individuals who have possession of them.

Associated Standard: NYS-S14-001, Information Security Risk Management Standard

4.11 Account Management and Access Control

a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT) unit.

b. Except as described in the ITS Policy NYS-S14-013, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned, unique identifiers known as user-IDs.

c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.

d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in NYS IT Policy NYS-S14-013, Account Management/Access Control Standard.

f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

g. Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (e.g., read, update, etc.).

i. Access privileges will be granted by the SE in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SE missions and business functions (i.e., least privilege).

j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for SE business or other approved use consistent with SE policy, and that user activities may be monitored and the user should have no expectation of privacy.

l. Advance approval for any remote access connection must be provided by the SE. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved, and the contractual, process, and technical controls required for such connection to take place.

m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

Working from a remote location must be authorized by SE management and practices which ensure the appropriate protection of SE data in remote environments must be shared with the individual prior to the individual being granted remote access. Working from international locations requires special legal, human resource, and security considerations and should only be allowed after careful SE analysis of these risks.

Associated Standards: NYS-S14-013, Account Management/Access Control Standard; NYS-S14-006, Authentication Tokens Standard; ; NYS-S20-001 Digital Identity Standard; NYS-S14-010 Remote Access Standard; NYS-S14-005, Security Logging Standard

4.12 Systems Security

a. Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of NYS. A list of assigned individuals or groups must be centrally maintained.
2. Information security must be considered at system inception and documented as part of the decision to create or modify a system.
3. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).
4. Each system must have a set of controls commensurate with the classification of any information that is stored on or passes through the system.
5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.

6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

    a. Databases and software (including in-house or third party developed and commercial off the shelf [COTS]):
        1. All software written for or deployed on SE systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
        2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
        3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
            i. All information security measures, including but not limited to access controls, system configurations, and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
            ii. sensitive data is masked or overwritten with fictional information.
        4. Where technically feasible, development software and tools must not be maintained on production systems.
        5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
        6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
        7. Privileged access to production systems by development staff must be restricted.
        8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

    b. Network Systems:

1. Connections between systems must be authorized by the executive management of all relevant SEs and protected by the implementation of appropriate controls.
2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to ensure:
    i. the business case for the connection is still valid and the connection is still required; and
    ii. the security controls in place (e.g., filters, rules, access control lists, etc.) are appropriate and functioning correctly.
3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    i. Internet accessible systems and internal systems;
    ii. systems with high security categorizations (e.g., mission critical, systems containing PPSI) and other systems; and
    iii. user and server segments.
4. Network management must be performed from a secure, dedicated network.
5. Authentication is required for all users connecting to State internal systems.
6. Network authentication is required for all devices connecting to State internal networks.
7. Only SE authorized individuals or business units may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the SE ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: NYS-S13-001, Secure System Development Lifecycle Standard; NYS-S13-002, Secure Coding Standard; NYS-S14-005, Security Logging Standard; NYS-S14-008, Secure Configuration Management Standard

4.13 Collaborative Computing Devices

a. Collaborative computing devices must:
    1. prohibit remote activation; and
    2. provide users physically present at the devices with an explicit indication of use.
b. SEs must provide simple methods to physically disconnect collaborative computing devices.

4.14 Vulnerability Management

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c. Penetration tests are required periodically for all critical environments/systems.

d. Where a SE has outsourced a system to another SE or a third party, vulnerability scanning/penetration testing must be coordinated.

e. Vulnerability scanning/penetration testing and mitigation must be included in third party agreements.

f. The output of the vulnerability scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for the evaluation of risk.

g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

Associated Standards: NYS-S15-001, Patch Management Standard; NYS-S15-002, Vulnerability Management Standard

4.15 Operations Security

a. All systems, and the physical facilities in which they are stored, must have documented operating instructions, management processes, and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. Any systems or services operated outside of CONUS must not connect to State networks or the State datacenter.

c. System configurations must follow approved configuration standards.

d. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

e. Where a SE provides a server, application, or network service to another SE, operational and management responsibilities must be coordinated by all impacted SEs.

f. Host based firewalls must be installed and enabled on all SE workstations to protect from threats and to restrict access to only that which is needed.

g. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across SE systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

h. Controls must be implemented to disable automatic execution of content from removable media.

i. Controls must be implemented to limit storage of SE information to SE authorized locations.

j. Controls must be in place to allow only SE approved software to run on a system and prevent execution of all other software.

k. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

l. All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.

m. Any system, software, or Operating System environment which is no longer supported and cannot be patched to current versions (e.g. end of life hardware/software) must be decommissioned and removed from service.

n. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and must record events to provide evidence and to reconstruct lost or damaged information.

o. Audit logs recording exceptions and other information security-relevant events must be produced, protected, and kept consistent with SE record retention schedules and requirements.

p. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.

q. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

r. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a minimum, these plans must include:

    1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

    2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

s. Backup copies of SE information, software, and system images must be taken regularly in accordance with SE defined requirements.

t. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

u. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: NYS-S14-008, Secure Configuration Management Standard; NYS-S14-005, Security Logging Standard; NYS-S13-005, Incident Response Standard; NYS-S14-013, Account Management/Access Control Standard

4.16 Citizens' Cyber Security Notification

a. All SEs are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with State Technology Law, Article II, Internet Security and Privacy Act.

b. Beyond the requirements of the Act, SEs must also notify non-NYS residents when there has been or is reasonably believed to have been a compromise of the individual's private information.

c. This policy also applies to information maintained on behalf of an SE by a third party.

d. The SE must consult with the CISO to help determine the scope of the breach and restoration measures.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs shall request an exception

through the CISO. Details regarding the exception process and the Exception Request Form can be found in ITS Policy, NYS-P13-001, Information Security Exception Policy.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The SE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-P03-002
NYS Office of Information Technology Services
1220 Washington Avenue, Bldg. 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

8.0 Revision History

This policy shall be reviewed at least once every two years to ensure relevancy.

Date	Description of Change	Reviewer
04/18/2003	Original Policy Release (*released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)*)	CIO/OFT
06/20/2014	Full revision	Deborah A. Snyder, Acting Chief Information Security Officer
09/19/2014	Added annual reporting requirement to Compliance section	Deborah A. Snyder, Acting Chief Information Security Officer
10/17/2014	Added bullet to Systems Security section to require security consideration at system inception; re-worded bullet on secure coding	Deborah A. Snyder, Acting

Date	Description of Change	Reviewer
		Chief Information Security Officer
02/20/2015	Added Collaborative Computing Devices section and definitions for collaborative computing and explicit indication; added links to associated standards for Vulnerability Management section	Deborah A. Snyder, Deputy Chief Information Security Officer
06/19/2015	Added EISO responsibility to monitor external sources for indications of breach, defacements, etc., removed hardware tagging requirement, clarified requirement for incident response plan, added definition of critical infrastructure.	Deborah A. Snyder, Deputy Chief Information Security Officer
05/04/2016	Changed NYS Cyber Incident Response Team (CIRT) to Cyber Command Center and updated email in Section 7.0	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update of contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/07/2018	Updated Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
09/20/2018	Corrected numbering in section 4.14	Deborah A. Snyder, Chief Information Security Officer
12/07/2018	Revised to clarify State Entity and workforce responsibilities to understand information security controls and to protect State information and resources, and personal, private, sensitive information, from unauthorized use or disclosure.	Deborah A. Snyder, Chief Information Security Officer
11/23/2021	Added language for CONUS and international work considerations, incorporated content from Security Controls standard, added Cyber Risk Coordinator description, and routine updates to remain consistent with other policy/standard changes.	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

International Standard ISO/IEC 27002, Information Technology – Security Techniques – Code of Practice for Information Security Controls

SANS Institute, Critical Security Controls for Effective Cyber Defense ("Top 20 Critical Security Controls")

State Technology Law, Article II, Internet Security and Privacy Act

Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies

Exhibit 1

Cyber Risk Coordinator Description

As outlined in Section 4.1., SEs must designate an individual or group to be responsible for cyber-related risk management. The Cyber Risk Coordinator (CRC) is the SE-assigned individual who ensures that cyber-related risk is managed within an SE. Organizations can implement this role either as a function of a current role (e.g., counsel, internal controls, etc.), or by creating a new role. The CRC must understand the SE's strategic goals and objectives. This individual should be either authorized to or made able to facilitate risk-based decision making, working with executive leadership. Where cyber security is a shared responsibility between SEs and ITS, the SE is responsible for managing security requirements and risk, by performing and/or participating in the following functions:

- Identification of critical assets
- Data classification
- Account management and control of agency resources
- Incident response and management
- Employee awareness and training
- Developing requirements for systems that support business functions
- Preparation and review of agency policies and procedures
- Disaster Recovery & Business Continuity planning
- Routine assessments where the SE must play a lead role (e.g., annual Nationwide Cyber Security Review)