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 Standard	**No:** NYS-S13-001
IT Standard: **Secure System Development Life Cycle**	**Updated:** 05/09/2024 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This Secure System Development Life Cycle (SSDLC) Standard defines security requirements that must be considered and addressed within every System Development Life Cycle (SDLC).

Computer systems and applications are developed/procured to address business needs. To do so effectively, system requirements must be identified early and addressed as part of the State Entity's (SE) SSDLC. Failure to identify a requirement until late in the process can have major repercussions to the success of a project and result in project delivery delays, deployment of an inadequate system, and even abandonment of the project. Furthermore, for each phase through which a project passes without identifying and addressing a requirement, the more costly and time-consuming it will become to fix problems that occur due to the omission.

Information security must be adequately considered and built into every phase of the SE's SSDLC. Failure to address risks and implement proper controls can result in inadequate security, potentially putting SEs, and the State at large, at risk of data breaches, reputational damage, loss of public trust, compromise to systems/networks, financial penalties, and legal liability.

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 standard applies to all "State Entities" (SE), defined as "State Government" in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any Information Technology (IT) Resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different policy/standard, it must include the requirements set forth in this one. Where a conflict exists between this standard and an SE's policy/standard, the more restrictive requirement will take precedence.

This standard covers all systems and applications developed/procured for New York State Entities (SEs), regardless of their current system life cycle phase. This includes all test, quality control, production and other ad-hoc systems that exist within or external to SE networks. This standard equally applies to systems developed by SE staff or by any third parties on behalf of the SE.

4.0 Information Statement

Per the NYS-P03-002: Information Security Policy, SEs must ensure an SSDLC is utilized in the development of all SE applications and systems, including applications and systems developed on behalf of SEs by contracted third-party partners.

The SE must ensure that, at a minimum, the following security activities are included in the SEs SSDLC and that these activities are documented or referenced within an associated information security plan. Documentation of SSDLC security activities must be sufficiently detailed to demonstrate the extent to which each security activity is applied, and all documentation must be retained by the SE for auditing purposes in accordance with applicable federal and state standards.

1. Classify Information and Establish a System Criticality Level
2. Establish Digital Identity Requirements

[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.

3. Create a System Profile and Decompose the System
4. Assess Risks
5. Select, Document, and Test Security Controls
6. Create Test Data
7. Perform Certification and Accreditation
8. Release & Maintenance Support
9. System Disposal

There is not necessarily a one-to-one correspondence between security activities and SSDLC phases. Security activities often need to be performed iteratively as a project progresses or cycles through the SSDLC. Unless stated otherwise, the placement of security activities within the SSDLC may vary in accordance with the SSDLC being utilized and the security needs of the application or system. Appendix A: Security Activities within the SDLC provides a sample correlation of security activities to a generic SDLC. Appendix B: Description of Security Activities provides a description of the above security considerations and activities.

Finally, it is important to note that the SSDLC process is intentionally comprehensive, to assure due-diligence, compliance, and proper documentation of security-related controls and considerations. Designing security into systems requires an investment of time and resources. The extent to which security is applied to the SSDLC process should be commensurate with the classification (data sensitivity and system criticality) of the system being developed and risks the system may introduce into the overall environment. This ensures value to the development process and deliverables. Generally speaking, the best return on investment is achieved by rigorously applying security within the SSDLC process to high risk/cost projects. Where it is determined that a project will not leverage the full SSDLC process – for example, on a lower-risk/cost project, the rationale must be documented, and the security activities that are not used must be identified and approved as part of the formal risk acceptance process.

Note: Data classification cannot be used as the sole determinate of whether the project is low risk/cost. For example, public facing websites cannot be considered low risk/cost projects even if all the data is public. Public facing websites may be subject to the risk of malware injections, compromise of visitor's machines, or alteration of website content, which could lead to reputational damage.

5.0 Compliance

This standard 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 standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this standard, 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-S13-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 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 document should be reviewed consistent with the requirements set forth in NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Date	Description of Change	Reviewer
10/18/2013	Original Standard Release	Thomas Smith, Chief Information Security Officer
10/17/2014	Added reference to identity assurance level requirements for NYS Identity Assurance (NYS-P10-006)	Deborah A. Snyder, Acting Chief Information Security Officer
03/10/2017	Updated Scope, Appendix headers, page numbering, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
05/09/2024	Streamlined the SSDLC Process and updated appendices	Chris DeSain, Chief Information Security Officer

9.0 Related Documents

NYS-S14-002, Information Classification Standard

NIST Special Publication 800-37, Rev 2, Risk Management Framework for

Information Systems and Organizations

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System ViewNIST Special Publication 800-30, Guide for Conducting Risk Assessments

NIST Special Publication 800-53, Rev 5, Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53A, Rev 5, Assessing Security and Privacy Controls in Information Systems and Organizations

NIST SP 800-160 Vol. 1, Rev. 1, Engineering Trustworthy Secure Systems

Appendix A: Security Activities within the SSDLC

There are many different industry accepted SDLC frameworks that can be used and researched. The actual placement of security activities may vary in accordance with the actual SDLC framework being utilized in a project, and the particular security needs of the application or system. There are also many other activities that may be included based on the framework used.

The table below illustrates the recommended placement of required security activities within the phases of a sample SDLC (Figure A-1). These are **examples** and therefore are not inclusive of all possible placements or activities.

In addition, many security activities are iterative and may extend between multiple phases. Appendix B contains description of each of the security activities in the standard.

Figure A-1: Recommended placement of Security Activities within SDLC Phases

Sample SDLC Phase	Security Activity
Initiation	• Classify Information • Establish System Criticality Level
Planning & Requirements Analysis	• Establish Digital Identity Requirements • Create a System Profile and Decompose the System
Design	• Create a System Profile and Decompose the System • Assess Risks • Select, Document, and Test Security Controls
Development	• Create a System Profile and Decompose the System • Assess Risks • Select, Document, and Test Security Controls
Integration & Testing	• Assess Risks • Select, Document, and Test Security Controls • Create Test Data
Implementation	• Assess Risks • Select, Document, and Test Security Controls
Operations & Maintenance	• Assess Risks • Perform Certification and Accreditation • Release & Maintenance Support

Sample SDLC Phase	Security Activity
Evaluation & Disposal	• Plan System Disposal

Appendix B: Description of Security Activities

1. Classify Information and Establish System Criticality

As per the NYS-P03-002: Information Security Policy, all information contained within, manipulated by, or passing through a system or application must be classified by the SE. Classification must reflect the importance of the information's confidentiality, integrity, and availability, as per the NYS-S14-002: Information Classification Standard. This will help determine minimum security controls, along with any legal and/or regulatory compliance domains.

The criticality of the system must be established and documented by the SE. The criticality level must reflect the business value of the function provided by the system and the potential business damage that might result from a loss of this functionality.

2. Establish Digital Identity Requirements

As per the NYS-P20-001: Digital Identity Policy, SEs must ensure all applications or systems which require authentication must establish an authorized account credential. Establishing digital identity requirements will ensure that access control of an application or system meets the requirements specified.

3. Create a System Configuration Profile and Decompose the System

The system or application being developed must be iteratively profiled by technical teams within the SSDLC. A system profile is a high-level overview of the system or application that identifies the system or application's attributes such as the physical topology, the logical tiers, components, services, actors, technologies, external dependencies, and access rights. This profile must be updated throughout the various phases of the SSDLC upon any changes to the design and/or architecture of the system or application. The system or application must be decomposed into finer components and its mechanics (i.e., the inner workings) must be documented. This activity is to be iteratively performed within the SSDLC. Decomposition should include production data flow and network diagrams to identify trust boundaries, information entry and exit points, data flows, and privileged functions.

4. Assess Risks

As per the NYS-S14-001: Information Security Risk Management Standard, SEs must iteratively perform risk assessments within the SSDLC process that include vulnerability scanning. Risk assessments begin as an informal, high-level process early in the SSDLC and will evolve throughout the life cycle of the development process. The result is a formal, comprehensive risk assessment process that is executed prior to placing a system or application into production.

All significant threats and vulnerabilities identified via risk assessments must be addressed by the SE, and SEs must appropriately manage all identified risks by avoiding, transferring, accepting, or mitigating the risk. Ignoring risk is prohibited. Risk assessments must adhere to all relevant state and federal mandates that the SE must document and be compliant with.

The risk assessments must be periodically reviewed and updated as necessary whenever the underlying risk assessment is modified or whenever significant changes are made to the system or application.

5. Select, Document, and Test Security Controls

Appropriate security controls must be implemented by SEs to mitigate risks that are not avoided, transferred, or accepted. Security controls must be justified and documented based on the risk assessments, threat assessments, and analysis of the cost of implementing a potential security control relative to the decrease in risk afforded by implementing the control.

Documentation of controls must be sufficiently detailed to enable verification of all systems and applications and the adherence to all federal compliance requirements such as FISMA, HIPAA, IRS Publication 1075, FERPA, etc.

Residual risk must be documented and maintained at acceptable levels by the SE. After mitigating controls have been implemented, a formal risk acceptance, with SE executive management sign-off, must be performed for all remaining medium and high risks.

All controls will be thoroughly tested and re-tested in pre-production environments that are identical, in as many ways as feasibly possible, to the corresponding production environment. This includes the hardware, software, system configurations, controls, and any other customizations.

Security control requirements must be periodically reviewed and updated as necessary whenever the system, application, or the underlying risk assessment is modified.

6. Create Test Data

A process for the development of significant test data must be created and documented by SEs for all systems and applications. A test process must be available for applications to perform security and regression testing (e.g., vulnerability scanning, static code analysis, red team/penetration testing).

Confidential production data should not be used for testing purposes. If production data is used, SEs must assess the risk of use and comply with all applicable federal, state, and external policies and standards regarding the protection and disposal of production data.

Associated Standards: NYS-S13-002: Secure Coding Standard; NYS-S14-005:

Security Logging Standard; NYS-S14-008: Secure Configuration Standard; NYS-P03-002: Information Security Policy.

7. Perform Certification and Accreditation

The information security plan must be analyzed, updated, and accepted by SE executive management. All systems and applications are required to undergo periodic risk assessments to ensure they reflect a security posture commensurate with each SEs definition of acceptable risk. Risk assessments must include assessments for compliance with all federal, state, and external compliance standards for which the SE is required to comply.

Risk assessments must be performed after all system and application changes, prior to deployment, and periodically as part of continuous system compliance monitoring.

8. Release & Maintenance Support

As part of the SSDLC process, the regular upkeep of systems is an important task. Throughout the life cycle of a system or application the following items will need to be considered: regular risk assessment reviews, final network diagrams, attachments of final scans prior to deployment, patch management plans, schedules of continued planning, and plans for OS upgrades and hardware refresh. This is not an all-inclusive list; however, it is important to know that when the system goes live, the iterative nature of the SSDLC process continues throughout its life cycle.

A formal change management process must be followed whenever a system or application is modified in order to avoid direct or indirect negative impacts that the change might impose. The change management process must ensure that all SSDLC security activities are considered and performed, if relevant, and that all SSDLC security controls and documentation that are impacted by the change are updated.

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

9. System Disposal

The information contained in systems and applications must be protected once a system or application has reached end of lifecycle and is no longer necessary to perform a SE function. Information must be retained, securely deleted or returned to the SE according to applicable federal and state mandates or other retention requirements. Information without retention requirements must be discarded or destroyed and all disposed media must be sanitized in accordance with applicable federal and state standards, including the NYS-S13-003: Sanitization Secure Disposal Standard, to remove residual information.