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**: | **Updated:** 03/10/17 |
| **Secure System Development Life Cycle** | **Issued By:** NYS Office of Information Technology Services<br><br>**Owner:** Enterprise Information Security Office |

## 1.0 Purpose and Benefits

While considered a separate process by many, information security is a business requirement to be considered throughout the System Development Life Cycle (SDLC). This Secure System Development Life Cycle Standard defines security requirements that must be considered and addressed within every SDLC.

Computer systems and applications are created to address business needs. To do so effectively, system requirements must be identified early and addressed as part of the SDLC. 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 the 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 is to fix problems that occur because of the omission.

Information security must be adequately considered and built into every phase of the SDLC. Failure to identify risks and implement proper controls can result in inadequate security, potentially putting New York State Entities at risk of data breaches, reputational exposure, loss of public trust, compromise to systems/networks, financial penalties and legal liability.

## 2.0 Authority

*Section 2 of Executive Order No. 117* provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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 is promulgated pursuant to New York State Information Technology Policy NYS-P03-002, Information Security, and applies to ITS, all State Entities (SE) that receive services from ITS, and affiliates of same (e.g., contractors, vendors, solution providers), which have access to or manage SE information. It also serves as recommended practice for the State University of New York, the City University of New York, non-Executive branch agencies, authorities, NYS local governments and third parties acting on behalf of same.

This standard covers all systems and applications developed 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 New York state staff or by any third parties on behalf of New York State.

## 4.0 Information Statement

Security is a requirement that must be included within every phase of a system development life cycle. A system development life cycle that includes formally defined security activities within its phases is known as a secure SDLC. Per NYS Information Security Policy, a secure SDLC must be utilized in the development of all SE applications and systems. This includes applications and systems developed for SEs.

At a minimum, an SDLC must contain the following security activities. These activities must be documented or referenced within an associated information security plan. Documentation must be sufficiently detailed to demonstrate the extent to which each security activity is applied. The documentation must be retained for auditing purposes.

1. Define Security Roles and Responsibilities
2. Orient Staff to the SDLC Security Tasks
3. Establish a System Criticality Level
4. Classify Information
5. Establish System Identity Assurance Level Requirements
6. Establish System Security Profile Objectives
7. Create a System Profile
8. Decompose the System
9. Assess Vulnerabilities and Threats
10. Assess Risks
11. Select and Document Security Controls

12. Create Test Data
13. Test Security Controls
14. Perform Certification and Accreditation
15. Manage and Control Change
16. Measure Security Compliance
17. Perform System Disposal

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

Finally, it is important to note that the Secure SDLC process is comprehensive by intention, 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 SDLC process should be commensurate with the classification (data sensitivity and system criticality) of the system being developed and risks this system may introduce into the overall environment. This assures value to the development process and deliverable. Generally speaking, the best return on investment is achieved by rigorously applying security within the SDLC process to high risk/high cost projects. Where it is determined that a project will not leverage the full Secure SDLC 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 or not 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. There is a risk of compromise of the website to inject malware and compromise visitor's machines or to change the content of the website to create embarrassment.

## 5.0 Compliance

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

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Enterprise 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.

| Term | Definition |
|---|---|
| **Authorization** | Access privileges granted to a user, program, or process or the act of granting those privileges. |
| **Data** | A subset of information in an electronic format that allows it to be retrieved or transmitted. |
| **Guideline** | Non-mandatory suggested course of action. |
| **Least Privilege** | Granting users, programs or processes only the access they specifically need to perform their business task and no more. |
| **Significant Change** | Includes but is not limited to:<br>• Adding/deleting/modifying features/functionality to existing systems;<br>• Substantial redesign of the existing system or environment; or<br>• Other modifications that could substantially affect the system security.<br>Exclusions include, but are not limited to changes to wording, adding links to an outside site, adding a document to a web site, installing vendor supplied security patches to the underlying software or operating system, or uploading data to the database. |

## 7.0 Contact Information

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

**Enterprise Information Security Office**
**Reference: NYS-S13-001**
**NYS Office of Information Technology Services**
**1220 Washington Avenue, Building 5**
**Albany, NY 12242**
**Telephone: (518) 242-5200**
**Email: EISO@its.ny.gov**

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

## 8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

| 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 |

## 9.0 Related Documents

Enterprise Project Management Office NYS Project Management Guidebook (PMG)

National Institute of Standards and Technology (NIST) Special Publication 800-64, Security Considerations in the System Development Life Cycle

NIST Special Publication 800-39 , Managing Information Security Risk: Organization, Mission & Information System View

NIST Special Publication 800-37, Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach

NIST Special Publication 800-30, Guide for Conducting Risk Assessments

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

NIST Special Publication 800-53A, Guide for Assessing Security Controls in Information Systems & Organizations: Building Effective Assessment Plans

Appendix A: Security Activities within the SDLC

The table below shows the placement of security activities within the phases of a sample SDLC. The actual placement of security activities within the system development life cycle may vary in accordance with the actual SDLC being utilized in a project and the particular security needs of the application or system. The NIST publications in the third column of this table are recommended documents to provide guidance in the placement and execution of security tasks within the system development life cycle. These documents are available from the NIST website (http://csrc.nist.gov/publications/PubsSPs.html).

Figure A-1: Placement of Security Activities within SDLC Phases

| NYS PMG SDLC Phase | Security Activity | NIST Publications |
|---|---|---|
| System Initiation | • Define Security Roles and Responsibilities<br>• Orient Staff on the SDLC Security Tasks<br>• Establish a System Criticality Level<br>• Classify Information (preliminary)<br>• Establish System Assurance Level Requirements<br>• Establish System Security Profile Objectives (preliminary)<br>• Create a System Profile (preliminary) | • SP800-12<br>• SP800-14<br>• SP800-35<br>• SP800-27<br>• SP800-47<br>• SP800-60<br>• SP800-63<br>• FIPS 199 |
| System Requirements Analysis | • Establish System Security Profile Objectives (iterative)<br>• Classify Information (iterative)<br>• Decompose the System (preliminary) | • SP800-23<br>• SP800-30<br>• SP800-36<br>• SP800-53<br>• SP800-55<br>• SP800-64<br>• FIPS 140-2 |
| System Design | • Create a System Profile (iterative)<br>• Decompose the System (iterative)<br>• Assess Vulnerabilities and Threats (preliminary)<br>• Assess Risks (preliminary)<br>• Select and Document Security Controls (preliminary) | |
| System Construction | • Create test data<br>• Assess Vulnerabilities and Threats (iterative)<br>• Assess Risks (iterative)<br>• Select and Document Security Controls (iterative)<br>• Test security controls | • SP800-35<br>• SP800-36<br>• SP800-37<br>• SP800-51<br>• SP800-53<br>• SP800-53A<br>• SP800-55<br>• SP800-56<br>• SP800-57<br>• SP800-61 |
| System Implementation | • Measure security compliance<br>• Document System Security Profile<br>• Document Security Requirements and Controls | |

| NYS PMG SDLC Phase | Security Activity | NIST Publications |
|---|---|---|
| System Acceptance | • Perform System Certification and Accreditation | • SP800-64 |
| Operations & Maintenance: | • Measure security compliance (periodic)<br>• Manage and control change<br>• Perform System Certification and Accreditation (iterative) | • SP800-26<br>• SP800-31<br>• SP800-34<br>• SP800-37<br>• SP800-53A<br>• SP800-55 |
| Disposition | • Preserve information<br>• Sanitize media<br>• Dispose of hardware and software | • SP800-12<br>• SP800-14<br>• SP800-35<br>• SP800-36<br>• SP800-64 |

Appendix B: Description of Security Activities

1. Define Security Roles and Responsibilities

Security roles must be defined and each security activity within the SDLC must be clearly assigned to one or more security roles. These roles must be documented and include the persons responsible for the security activities assigned to each role. Appendix C: Security Roles within the SDLC provides guidelines for defining security roles and assigning security activities to roles.

2. Orient Staff to the SDLC Security Tasks

All parties involved in the execution of a project's SDLC security activities must understand the purpose, objectives and deliverables of each security activity in which they are involved or for which they are responsible.

3. Establish System Criticality Level

When initiating an application or system, the criticality of the system must be established. 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 access to this functionality.

4. Classify Information

As per NYS Information Security Policy, all information contained within, manipulated by or passing through a system or application must be classified. Classification must reflect the importance of the information's confidentiality, integrity and availability.

5. Establish System Identity Assurance Level Requirements

As per the NYS Information Assurance Policy, all applications or systems which require authentication must establish a user identity assurance level. The identity assurance level must reflect the required confidence level that the person seeking to access the system is who they claim to and the potential impact to the security and integrity of the system if the person is not who they claim to be.

6. Establish System Security Profile Objectives

When initiating an application or system, the security profile objectives must be identified and documented. These objectives must state the importance and relevance of identified security concepts (Appendix D: Security Concepts) to the system and indicate the extent and rigor with which each security concept is to be built in or reflected in the system and software. Each security concept must be considered throughout each life cycle phase and any special considerations or needs documented.

The purpose behind establishing system security profiles and monitoring them throughout the lifecycle is to be actively aware of the relative priority, weight and relevance of each security concept at each phase of the system's life cycle. SE's must verify that the security

profile objectives adequately consider all federal, state and external security mandates for which the system must be compliant.

7. Profile the System

The system or application being developed must be iteratively profiled by technical teams within the SDLC. A system profile is a high-level overview of the application that identifies the 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 SDLC.

8. Decompose the System

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 SDLC. Decomposition includes identifying trust boundaries, information entry and exit points, data flows and privileged code.

9. Assess Vulnerabilities and Threats

Vulnerability assessments must be iteratively performed within the SDLC process. Threat assessments must consider not only technical threats, but also administrative and physical threats that could have a potential negative impact on the confidentiality, availability and integrity of the system. Threat assessments must consider and document the threat sources, threat source motivations and attack methods that could potentially pose threats to the security of the system.

Threat assessments must adhere to all relevant state and federal mandates to which the SE must comply and follow industry best practices including the documentation of the assessment processes. Threat assessments and the underlying threat modeling deliverables that support the assessment must also be fully documented. Appendix E: Threat and Risk Assessment Resources includes a list of recommended resources for performing threat assessments.

10. Assess Risk

Risk assessments must be iteratively performed within the SDLC process. These begin as an informal, high-level process early in the SDLC and become a formal, comprehensive process prior to placing a system or software into production.

All realistic threats and vulnerabilities identified in the threat assessments must be addressed in the risk assessments. The risk assessments must be based on the value of the information in the system, the classification of the information, the value of the business function provided by the system, the potential threats to the system, the likelihood of occurrence, the impact of the failure of the system and the consequences of the failure of security controls.

All identified risks are to be appropriately managed 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.

The risk assessments must be periodically reviewed and updated as necessary whenever the underlying threat assessment is modified or whenever significant changes are made to the system. Appendix E: Threat and Risk Assessment Resources includes a list of recommended resources for performing risk assessments.

11. Select and Document Security Controls

Appropriate security controls must be implemented 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 that all systems and applications adhere to all relevant security policies and to respond efficiently to new threats that may require modifications to existing controls.

Residual risk must be documented and maintained at acceptable levels. A formal risk acceptance, with executive management sign-off, must be performed for medium and high risks that remain after mitigating controls have been implemented.

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

12. Create Test Data

A process for the development of significant test data must be created for all applications. A test process must be available for applications to perform security and regression testing.

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

13. Test Security Controls

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

The testing process, including regression testing, must demonstrate that all security controls have been applied appropriately, implemented correctly and are functioning properly and actually countering the threats and vulnerabilities for which they are intended. The testing process must also include vulnerability testing and demonstrate the remediation of critical vulnerabilities prior to placing the system into production.

Appropriate separation of duties must be observed throughout the testing processes such as ensuring that different individuals are responsible for development, quality assurance and accreditation.

14. Perform Accreditation

The system security plan must be analyzed, updated, and accepted by SE executive management.

15. Manage and Control Change

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 SDLC security activities are considered and performed, if relevant, and that all SDLC security controls and documentation that are impacted by the change are updated.

16. Measure Security Compliance

All applications and systems are required to undergo periodic security compliance assessments to ensure they reflect a security posture commensurate with each SEs definition of acceptable risk. Security compliance assessments must include assessments for compliance with all federal, state and external compliance standards for which the SE is required to comply.

Security compliance assessments must be performed after all system and application changes and periodically as part of continuous system compliance monitoring.

17. Perform System Disposal

The information contained in applications and systems must be protected once a system has reached end of life. Information must be retained 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 to remove residual information.

# Appendix C: Security Roles within the SDLC

Responsibility for each security activity within the SDLC must be assigned to one or more security roles. To accomplish this, the default definition of an SDLC role may be expanded to include security responsibilities and/or new security roles may be defined to encompass security activities. In all cases, the assignment of security activities to roles, and the identification of persons given responsibility for these roles, must be clearly documented.

For the purpose of utilizing a consistent definition of roles across various SDLC's, it is highly recommended that SE's utilize as guidelines the New York State Office of Information Technology Services (ITS) Enterprise Program Management Office (EPMO) and the National Institute of Standards and Technology (NIST) publications . Of specific relevance to the definition of roles and SDLC frameworks are:

- EPMO NYS Project Management Guidebook (PMG)
- NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle

The makeup of a system and software from a security perspective is its security profile and includes the following security concepts, which must be considered and documented as part of a Secure SDLC process.

Figure D-1: Security Concepts

| Concept | Description |
|---|---|
| Confidentiality | Protect against unauthorized information disclosure |
| Integrity | Protect against unauthorized, unintentional or incorrect modification of software or data. |
| Availability | Ensure the availability of systems and information. |
| Authentication | The process of establishing confidence in the identity of users or information systems. |
| Authorization | Establish access rights to resources. |
| Auditing/Logging | Build a historical record of user actions and of critical system processes. |
| Session Management | Ensure that a session maintains the confidentiality and integrity of the information exchanged between a system and an authenticated user. |
| Errors and Exception Management | Ensure that unintended and unreliable system behavior is securely handled. This helps ensure protection against confidentiality, integrity and availability threats. |
| Configuration Parameters Management | Ensure that the configurable parameters that are needed for software or a system to run are adequately protected. |
| Least Privilege | Assign only the minimum allowable rights to a subject that requests access to a resource for the shortest duration necessary. |
| Separation of Privilege | Ensure that multiple conditions are met before granting permissions to an object. |
| Defense in Depth | Layer security defenses in an application to reduce the chance of a successful attack. |
| Failing Securely | Ensure the confidentiality and integrity of a system remains intact even though system availability has been lost due to a system failure. |
| Economy of Mechanisms | Keep the system implementation and design as simple as possible. |
| Complete Mediation | Require access checks to an object each time a subject requests access, especially for security-critical objects. |
| Open Design | Use real protection mechanisms to secure sensitive information; do not rely on an obscure design or implementation to protect information (otherwise known as “security through obscurity”). |
| Least Common Mechanisms | Avoid having multiple subjects share mechanisms to grant access to a resource. |
| Psychological Acceptability | Ensure that security functionality is easy to use and transparent to the user. |

| Concept | Description |
|---|---|
| Leveraging Existing Components | Promote the reusability of existing components. Reuse proven and validated code and standard libraries rather than creating custom code. |
| Weakest Link | Identify and protect a system's weakest components. |
| Single Point of Failure | Eliminate any single source of complete compromise. |

Information concerning these concepts is publically available at the US Department of Homeland Security (DHS) Office of Cyber Security and Communications sponsored website at https://buildsecurityin.us-cert.gov.

In order to assure alignment with business compliance mandates, and help assure efficient and effective delivery of security services, the use of industry-recognized standards related to risk-based frameworks and secure system development life cycle practices are recommended.

In particular, the use of NIST standards is highly recommended, especially for SEs required to comply with federal security mandates. The following NIST publications provide recommended guidance for implementing risk management frameworks and performing threat and risk assessments.

- NIST Special Publication 800-39 , Managing Information Security Risk: Organization, Mission & Information System View
- NIST Special Publication 800-37, Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach
- NIST Special Publication 800-30, Guide for Conducting Risk Assessments
- NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53A, Guide for Assessing Security Controls in Information Systems & Organizations: Building Effective Assessment Plans

NIST publications are available at the National Institute of Standards and Technology website (http://csrc.nist.gov/publications/PubsSPs.html).