**Template Instructions**

Secure Configuration Standard

Follow the instructions below to complete this policy template for use within your own organization.

1. Click each bracketed field below to input basic policy information:

* **Organization Name *(e.g. ACME Co)*:**

[Organization Name]

* **Organization Address *(e.g. 123 Elm St. City, ST. 12345)*:**

[Organization Address]

* **Policy Authority *(e.g. CEO, CIO, or CISO)*:**

[Policy Authority]

* **Policy Owner *(e.g. IT Department)*:**

[Policy Owner]

* **Owner Contact Info *(e.g.*** [***jon.smith@acme.com***](mailto:jon.smith@acme.com)***)*:**

[Owner Contact Info]

* **Policy Number *(e.g. IT POL-INFOSEC-01)*:**

[Policy Number]

1. Thoroughly review all 10 Policy Sections to ensure accuracy and alignment with existing organizational policies and procedures.
2. Input key term definitions that require clarification into Section 7.
3. Review related documents in Section 10.
4. Save the document and print the necessary pages to a PDF or printer.
5. Visit [docs.policytemplates.online](https://docs.policytemplates.online/) for further policy creation and implementation resources.

|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Secure Configuration** | **Updated:** 10/31/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# Purpose and Benefits

The Secure System Development Life Cycle (SDLC) Standard integrates information security as a core requirement throughout the SDLC, ensuring that security considerations are identified and addressed at every phase. This approach aligns security measures with business needs, enhancing the overall integrity of the systems being developed. By embedding security from the outset, the standard aims to create robust systems that effectively meet organizational objectives.

Identifying security requirements early in the SDLC provides several benefits. It mitigates risks associated with data breaches and system compromises, reduces costs by preventing expensive fixes and project delays, and promotes timely project delivery while ensuring systems perform as intended. Furthermore, by safeguarding sensitive information, the standard protects the organization’s reputation and minimizes potential legal liabilities, fostering public trust in the organization's commitment to security.

# 2.0 Authority

This standard is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This standard applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The standard encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Secure Configuration Standard outlines guidelines for configuring and managing information systems at [Organization Name] to enhance security and compliance. It requires the use of industry consensus guidelines, such as CIS Benchmarks, NIST Checklists, and USGCB, as the basis for secure configuration profiles. Any modifications must be justified by business needs, developed with input from the Information Security Officer, and documented for audit purposes. Initial setups and configurations must occur in a secure environment, with changes following a formal process that includes review and security impact analysis. Configuration management plans must be maintained to align with secure system development life cycle practices. Ongoing monitoring is essential to detect unauthorized changes, misconfigurations, and vulnerabilities, ensuring systems remain secure over time.

* 1. Industry Standards

Standard secure configuration profiles, based on any one or more of the industry consensus guidelines listed below, must be used in addition to the latest vendor security guidance. Alterations to the profile must be based on business need, policy or standard compliance, developed in consultation with the Information Security Officer/designated security representative, documented and retained for audit purposes.

Industry Consensus Guidelines:

1. [Center for Internet Security (CIS) Benchmarks](http://benchmarks.cisecurity.org/)
2. [National Institute of Science and Technology (NIST) National Checklist Program](http://web.nvd.nist.gov/view/ncp/repository)
3. [United States Government Configuration Baselines (USGCB)](http://usgcb.nist.gov/usgcb_content.html)
   1. Secure Environment

The initial setup, software installation, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.

* 1. Changes

Changes to configurations are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the change management procedures. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

* 1. Management

Entities must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

* 1. Monitoring

A configuration monitoring process must be in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.

# 5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended 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, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this standard must be submitted to the [Policy Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Policy Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

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

[Policy Owner]

[Owner Contact Info]

[Organization Address]

# 9.0 Review and Revision

This standard should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[NIST Special Publication 800-30, Guide for Conducting Risk Assessments](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final" \t "_blank)

[NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations](https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news" \t "_blank)

[NIST Special Publication 800-53A, Guide for Assessing Security Controls in Information Systems & Organizations: Building Effective Assessment Plans](https://www.nist.gov/publications/guide-assessing-security-controls-federal-information-systems-and-organizations)

**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 * Orient Staff on the SDLC Security Tasks * Establish a System Criticality Level * Classify Information (preliminary) * Establish System Assurance Level Requirements * Establish System Security Profile Objectives (preliminary) * Create a System Profile (preliminary) | * SP800-12 * SP800-14 * SP800-35 * SP800-27 * SP800-47 * SP800-60 * SP800-63 * FIPS 199 |
| System Requirements Analysis | * Establish System Security Profile Objectives (iterative) * Classify Information (iterative) * Decompose the System (preliminary) | * SP800-23 * SP800-30 * SP800-36 * SP800-53 * SP800-55 * SP800-64 * FIPS 140-2 |
| System Design | * Create a System Profile (iterative) * Decompose the System (iterative) * Assess Vulnerabilities and Threats (preliminary) * Assess Risks (preliminary) * Select and Document Security Controls (preliminary) |
| System Construction | * Create test data * Assess Vulnerabilities and Threats (iterative) * Assess Risks (iterative) * Select and Document Security Controls (iterative) * Test security controls | * SP800-35 * SP800-36 * SP800-37 * SP800-51 * SP800-53 * SP800-53A * SP800-55 * SP800-56 * SP800-57 * SP800-61 * SP800-64 |
| System Implementation | * Measure security compliance * Document System Security Profile * Document Security Requirements and Controls |
| System Acceptance | * Perform System Certification and Accreditation |
| Operations & Maintenance: | * Measure security compliance (periodic) * Manage and control change * Perform System Certification and Accreditation (iterative) | * SP800-26 * SP800-31 * SP800-34 * SP800-37 * SP800-53A * SP800-55 |
| Disposition | * Preserve information * Sanitize media * Dispose of hardware and software | * SP800-12 * SP800-14 * SP800-35 * SP800-36 * 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](#AppendixC) provides guidelines for defining security roles and assigning security activities to roles.

1. 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.

1. 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.

1. Classify Information

As per the 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.

1. Establish System Identity Credential Requirements

All applications or systems which require authentication must establish a user identity credential. The identity credential 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.

1. 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](#AppendixD)) 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. Entities must verify that the security profile objectives adequately consider all federal, state and external security mandates for which the system must be compliant.

1. 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.

1. 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.

1. 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 entity 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](#AppendixE) includes a list of recommended resources for performing threat assessments.

1. 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 entity 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](#AppendixE) includes a list of recommended resources for performing risk assessments.

1. 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.

1. 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, entities must comply with all applicable federal, state and external policies and standards regarding the protection and disposal of production data.

1. 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.

1. Perform Accreditation

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

1. 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.

1. Measure Security Compliance

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

1. 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 entities utilize as guidelines the National Institute of Standards and Technology (NIST) publications . Of specific relevance to the definition of roles and SDLC frameworks are:

* [NIST Special Publication 800-37 Rev. 2 Risk Management Framework for Informtion Systems and Organizations: A System Life Cycle Approach for Security and Privacy](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)

**Appendix D: Security Concepts**

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. |
| 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>.

**Appendix E: Threat and Risk Assessment Resources**

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 entities 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](https://csrc.nist.gov/publications/detail/sp/800-39/final)
* [NIST Special Publication 800-37 Rev. 2 Risk Management Framework for Informtion Systems and Organizations: A System Life Cycle Approach for Security and Privacy](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)
* [NIST Special Publication 800-30, Guide for Conducting Risk Assessments](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final" \t "_blank)
* [NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations](https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news)
* [NIST Special Publication 800-53A, Guide for Assessing Security Controls in Information Systems & Organizations: Building Effective Assessment Plans](https://www.nist.gov/publications/guide-assessing-security-controls-federal-information-systems-and-organizations)

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