Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Secure System and Software Life Cycle Management Standard

Document Name: Secure System and Software Life Cycle Management Standard	Effective Date: October 15th, 2018
Document ID: IS.025	Last Revised Date: March 11, 2025

Table of Contents

1. PURPOSE

1.1. This **standard** establishes requirements for identifying **controls** that will be incorporated in system and **software** planning, design, building, testing and implementation, including:

1.1.1. **Information** security activities that will occur during the system and **software** development life cycle.

1.1.2. Required **controls** for supporting system or **software** development **processes** such as segregation of environments, prevention and/or protection of **confidential** production **data** in test environments.

1.1.3. The use of version **control** for **software** development.

1.1.4. Requirements for security hardening when building and configuring systems and **applications**.

2. AUTHORITY

2.1. Pursuant M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possess the authority to establish **policies**, **procedures**, and objectives with respect to activities concerning **information** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of **information**, **information systems**, **assets**, **applications**, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, **agencies**, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement **procedures** that ensure their **personnel** comply with the requirements herein to safeguard **information**.

4. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this *standard*. The Enterprise Risk Management Office is responsible for this *standard* and may enlist other departments to assist in maintaining and monitoring compliance with this *standard*. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this *standard* on an annual basis, or when significant *policy* or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. Additional ***information*** regarding this *standard* and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/policies.

4.3. In the event of any conflict between the provisions contained in this *standard* and the provisions set forth in any of the Enterprise Information Security Policies, the provisions in the Enterprise Information Security Policies will govern.

4.4. Definitions of terms in bold may be found in the ***IS.Glossary of Terms*** at https://www.mass.gov/cybersecurity/***policies***.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth**.**

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance.

5.3.2. Identify and explain in detail the *risks* created due to the non-compliance.

5.3.3. Provide a detailed explanation of the *controls* the agency, or office will implement to mitigate the *risks* to an acceptable level.

5.3.4. Specify the time-frame required to implement the *controls* and mitigate the identified *risks*. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the *risk owner* and the *control owner* designated by the agency to accept and manage the *risks* associated with the non-compliance and implement the *controls* that will effectively mitigate the identified *risks.*

6. STANDARD STATEMENTS

6.3. Security in System and Software Life Cycle

6.3.1. Commonwealth Agencies and Offices must define and oversee a *process* for addressing security and privacy *risks* throughout the systems development and acquisition life cycles.

6.3.2. Commonwealth Agencies and Offices must follow a *risk*-based approach in determining the appropriate level of security based on the criticality or sensitivity of the system under consideration (see *IS.021 Information Security Risk Management Standard).*

6.3.3. Security considerations will be included in the plan, design, build, test and implementation phases of the system and *software* life cycle.

6.3.4. Plan and Scope

6.3.4.1. Initial *Risk* Analysis

6.3.4.1.1. At the earliest opportunity during the design and development phase, a high-level *risk* assessment will be performed by the **Information Owner** or designee, with support from the agency's *information* security *personnel*.

6.3.4.1.2. The high-level *risk* assessment will include all significant changes where security or privacy is applicable, including, but not limited to:

6.3.4.1.2.1. New *software applications.*

6.3.4.1.2.2. New *software* features.

6.3.4.1.2.3. Introduction of new system and *software* architecture or a significant modification to existing *software application* features or existing architecture, (see *IS.021 Information Security Risk Management Standard).*

6.3.4.1.3. This initial *risk* assessment should determine whether or not the proposed system or *software* can operate within the agency's *risk* profile and identify the initial set of key *controls*

that should be implemented to mitigate any major concerns.

6.3.4.2.   Security Requirements Definition

6.3.4.2.1. Based on the initial *risk* assessment, security-related requirements for the proposed system and/or *software* will be identified, validated, and incorporated into the design, and approved by the **Information Owner**.

6.3.4.2.2. Leading industry security standards and best practices will be used as a reference, such as NIST, OWASP Top 10 and CIS, to provide a comprehensive list of initial requirements for consideration.

6.3.4.2.3. The security requirements will be refined and supplemented throughout the lifecycle of the system or *software*, based on supplemental detailed *risk* assessments.

6.3.5. Design

6.3.5.1.   To ensure that security is incorporated in the system and *software* life cycle, the system design will include a "security-as-a-design" objective, and any security exceptions will be identified by the **Information Owner** or **Information Custodian**.

6.3.5.2.   Security Design

6.3.5.2.1. The **Information Owner** and **Information Custodian** will address all high-*risk* security-related requirements identified during project planning. In addressing these requirements, the following will be performed:

6.3.5.2.1.1.   Architecture: Develop design specification and/or security architecture that describes the approach to protecting the confidentiality, integrity, and availability of the system. New architecture should integrate enterprise architecture standards.

6.3.5.2.1.2.   Test Plans: Test plans must be in place for validating security testing requirements. The following tests must be performed as applicable:

6.3.5.2.1.2.1. Threat assessments based on functional requirements.

6.3.5.2.1.2.2. Classification of the *data* involved.

6.3.5.2.1.2.3. Security requirements gathering and documentation.

6.3.5.2.1.2.4. System design reviews for security.

6.3.5.2.1.2.5. Secure code reviews.

6.3.5.2.1.2.6. Penetration testing.

6.3.5.2.1.2.7. **Vulnerability** scanning.

6.3.5.2.1.2.8. Host and/or network configuration reviews.

6.3.5.2.1.2.9. **Third-party** security reviews (design reviews, code reviews, testing, etc.)

6.3.5.2.1.3. <u>Security Design Review</u>: Security **personnel** will review the security design for all high-**risk** security requirements when conducting design reviews prior to build, test, and implementation.

6.3.6. Build

6.3.6.1. Depending on the methodology in use (e.g., waterfall, agile, scrum), security tollgates must be incorporated to ensure secure development.

6.3.7. Test

6.3.7.1. To ensure and validate that security is incorporated in the system and **software** life cycle, the following testing is required:

6.3.7.1.1. <u>Identification and Testing of Security **Controls**</u>: **Information Owners** and **Information Custodians** will test security requirements prior to implementation and use. For **software**, the following will be performed:

6.3.7.1.1.1. Automated source code scanning (static analysis) of all supported code should be performed using a Commonwealth-approved code analysis tool.

6.3.7.1.1.2. Manual source code analysis should be performed on all **information system** source code during testing and prior to deployment.

6.3.7.2. Documentation of Change

6.3.7.2.1. Any changes to systems and **software** will be approved in line with change and release management **procedures**.

6.3.7.2.2. Change records will be made available to security **personnel** for review when required.

6.3.8. Implementation

6.3.8.1. To ensure that security is incorporated in the system and **software** life cycle, the implementation will include **processes** for validation and change **control**.

6.3.8.1.1. Validation

6.3.8.1.1.1. **Information Owners** and **Information Custodians** will ensure that new or significantly changed systems and **software applications** are released to the production environment only after a pre-implementation security **risk** assessment and **information** security issues are addressed.

6.3.8.1.2. Change Control

6.3.8.1.2.1. Changes related to Commonwealth **information systems** and **software** will be approved by the respective Change Advisory Board (s*ee Change Management in IS.023 Operations Management Standard*) prior to release to production environments (e.g., such as the completion of successful test simulations and resolution of identified issues where applicable).

6.3.8.1.2.2. Ensure appropriate security **controls** are in place before approving the change in level for the code.

6.3.8.1.2.3. Changes that alter the security **controls** in place at the **application**, system or network level will be reviewed prior to release to production.

6.3.8.2. All source code and configurations will be checked into an approved code repository.

6.3.9. Maintenance

6.3.9.1. Commonwealth Agencies and Offices must ensure that **Information Owners** coordinate with Security Officers and the Enterprise Security Office to deploy security patches/updates in a timely fashion to resolve **vulnerabilities** while ensuring the full functionality of the **information system** (*see IS.027 Vulnerability Management Standard*).

6.3.10. Decommissioning

6.3.10.1. Prior to decommissioning, the **Information Owner** will formalize plans describing the **processes** to securely remove, archive, or protect **sensitive data** from the systems to be decommissioned (see *Information Disposal in IS.015 Asset Management Standard*).

6.4. Security in SDLC Support Processes

6.4.1. Commonwealth Agencies and Offices must ensure that **controls** are implemented to ensure that the resources, materials, and **procedures** used in the development **process** are managed to minimize the introduction of security **vulnerabilities**.

6.4.2. In the event of an **information** spill or **data breach**, the Incident Response Plan will be initiated.

6.4.3. Control Application Software

6.4.3.1. The following is required for maintaining **application software**:

6.4.3.1.1. <u>Change Control Processes</u>: All changes to system components must follow the change management process (*see IS.023 Operations Management Standard)*.

6.4.3.1.2. <u>Segregation of Environments</u>: Development, test, and production environments will be separated to reduce the **risks** of unauthorized access or changes to production systems and code repositories. Commonwealth Agencies and Offices will adhere to the following rules:

6.4.3.1.2.1. Rules for the transfer of **software** from development to production status will be logged through a formal recordkeeping system (*see IS.023 Operations Management Standard*).

6.4.3.1.2.2. Development, test, and production **software** will run on different systems or computer processors.

6.4.3.1.2.3. **Access controls** must be used to enforce access to the development, test, and production environments.

6.4.3.1.2.4. Test environments must emulate the operating system environment as closely as possible.

6.4.3.1.2.5. **Confidential** production **data** should not be copied into the test environment.

6.4.3.1.2.6. Test *data* must be removed from systems prior to going live in the production environment.

6.4.3.2. Secure Coding Practice

6.4.3.2.1. ***Applications*** must be developed using secure coding practices to prevent common coding ***vulnerabilities*** in ***software*** development ***processes*** (e.g., OWASP Top 10) to include, but not limited to, the following:

6.4.3.2.1.1. Injection flaws (e.g., SQL injection, OS Command Injection, LDAP, and XPath injection flaws as well as other injection flaws).

6.4.3.2.1.2. Broken authentication and session management.

6.4.3.2.1.3. Cross-site scripting (XSS) .

6.4.3.2.1.4. Broken access ***control*** (e.g., insecure direct object references, failure to restrict URL access and directory traversal) .

6.4.3.2.1.5. Security misconfiguration.

6.4.3.2.1.6. ***Sensitive data*** exposure.

6.4.3.2.1.7. Insufficient attack protection (i.e., ability to detect, prevent and respond to both manual and automated attacks).

6.4.3.2.1.8. Cross-site request forgery (CSRF).

6.4.3.2.1.9. Using Components with known ***vulnerabilities*** (e.g., libraries, ***software*** modules).

6.4.3.2.1.10. Unprotected APIs (e.g., JavaScript in the browser and mobile apps that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT)).

6.4.3.2.1.11. Others, including buffer overflow, insecure ***cryptographic*** storage, improper error handling.

6.4.3.3. Custom Application Accounts, User IDs and Passwords

6.4.3.3.1. Default or custom ***application*** accounts, ***user*** IDs and passwords will be removed before systems are moved into production (see *User Access Management in IS.014 Access Management Standard)*.

6.4.4. Release Management Process

6.4.4.1. Releasing new systems and **application software** to the production environment must follow a defined process that ensures the integrity and accountability of all of the components released.

6.4.4.2. Systems and **applications** will not be released to the production environment until use case testing is completed and recorded in source code or configuration change repositories.

6.4.5. Vendor Software Maintenance

6.4.5.1. Vendor-supplied **software** (e.g., product upgrades, updates, and patches; **software** developed by **third parties**) must be updated and maintained to ensure reduced **risk** of security **vulnerabilities**.

6.4.5.2. Change **control procedures** will be documented according to the change and release management **procedures**.

6.4.6. Protection of Data Integrity

6.4.6.1. The **Information Custodian** is responsible for ensuring system inputs, outputs and processing functions are validated prior to production release in coordination with the development team.

6.4.7. Protection of System Test Data

6.4.7.1. The following is required for protecting system test **data**:

6.4.7.1.1. Authorization: The use of **confidential** production **data** in a non-production environment is prohibited unless required for a business purpose and explicitly approved by the **Information Security Team** (see *Release Management in IS.012 Operations Management Standard)*.

6.4.7.1.2. Data Masking: The use and copying of **confidential** production **data** is prohibited unless masking routines or other protective measures are applied to protect the **confidential** production **data** from unauthorized disclosure.

6.4.7.1.3. Secure Data Storage and Removal: The storage of **confidential** production **data** used in the development environment will adhere to the *Information Protection* requirements of *IS.015 Asset Management Standard*. **Confidential** production **data** will be removed from test systems when it is no longer required.

6.4.8. Protection of Application Source Library

6.4.8.1. The following are required for protecting **application** source libraries:

6.4.8.1.1. <u>Version Control</u>: Old versions of production **application** source libraries will be archived using version **control**. Version controlled archives will contain summary **information**, including, but not limited to, version numbers and date of last use.

6.4.8.1.2. <u>Protection From Covert Channels and Malicious Code</u>: The creation of covert channels or administrative "back doors" in a system and/or **software** and its release into the production environment is strictly prohibited. A channel may be considered covert or an administrative "back door" if it allows remote access functionality that was not intended in the **software** design specifications.

6.5. System Hardening

6.5.1. Commonwealth Agencies and Offices must ensure that operating systems for email, **application**, web, database, network devices and file servers are hardened to protect against exploitation from non-authorized or malicious use.

6.5.2. Adherence to hardening standards to protect and secure Commonwealth **information assets** prior to deployment into production environments is mandatory.

6.5.3. Risk Assessments

6.5.3.1. **Information Owners** will perform **risk** assessments on a regular basis to determine if existing/planning **controls** adequately meet the criticality and sensitivity of the **information asset**. More restrictive **controls** may be implemented as needed.

6.5.4. Technical Security **Standards**

6.5.4.1. Technical security **standards** will be developed for all critical and high-**risk information systems**.

6.5.4.2. These **standards** will address known security **vulnerabilities** and must be consistent with industry-accepted system hardening standards.

6.5.4.3. It is the responsibility of **application** and platform owners in collaboration with the Enterprise Security Office to develop

technical **standards** for critical and high-**risk** systems that they own or support.

6.5.4.4. Review of technical **standards**

6.5.4.4.1. Systems will be reviewed periodically for compliance with technical **standards** by **Information Custodians**, **information** security **personnel** or the appropriate designee to ensure regular compliance:

6.5.4.4.1.1. **Information Custodians** are responsible for ensuring and maintaining compliance with technical **standards**.

6.5.4.4.1.2. **Information Security Teams** are responsible for monitoring and measuring compliance with technical **standards**.

6.5.5. Primary System Function

6.5.5.1. Implement only one primary function per server (or virtual server) to prevent functions that require different security levels from coexisting on the same server (e.g., web servers, database servers, DNS).

6.5.6. Patch Management

6.5.6.1. Apply the most up-to-date vendor-supplied security patches or upgrades to correct for known **vulnerabilities**.

6.5.6.2. Security patches should be deployed in a timely manner and consistent with the patch deployment schedule defined in *IS.027 Vulnerability Management Standard*.

6.5.6.3. Any known **vulnerabilities** with the OS will be remediated (or a **risk exception** must be requested and approved) accordingly before using it to host a server.

6.5.7. Disabling or Removing Unnecessary Services

6.5.7.1. Disable or remove service, **applications** and network protocols that are not required when configuring the OS.

6.5.7.2. Minimal OS configurations will be installed, and services, **applications** and network protocols will be added as needed for business purposes.

6.5.7.3. Common types of services and **applications** that should be removed include but are not limited to:

6.5.7.3.1. File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], FTP).

6.5.7.3.2. Wireless networking services.

6.5.7.3.3. Remote control and remote access programs, particularly those that do not strongly *encrypt* their communications (e.g., Telnet).

6.5.7.3.4. Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS]).

6.5.7.3.5. Web servers and services.

6.5.7.3.6. Unnecessary scripts and drivers.

6.5.7.3.7. Unnecessary subsystems and file systems.

6.5.7.3.8. Email services (e.g., SMTP).

6.5.7.3.9. Language compilers and libraries.

6.5.7.3.10. System development tools.

6.5.7.3.11. System and network management tools and utilities, including Simple Network Management Protocol (SNMP).

6.5.8. Disabling or Removing Default Accounts

6.5.8.1. Operating system account defaults will be reviewed and updated by removing or disabling account default configurations (*see Account Management in IS.014 Access Management Standard*). **Controls** for *user* authentication include but are not limited to:

6.5.8.1.1. Disable or remove interactive default accounts. For default accounts that need to be retained, restrict access, and change the name (where possible) and default password.

6.5.8.1.2. Disable or remove non-interactive (e.g., system) accounts and their associated passwords.

6.5.9. Configuring System Security Parameters

6.5.9.1. System security parameters will be configured to prevent misuse.

6.5.9.2. System administrators and security resources should be knowledgeable of common security parameter settings for system components.

6.5.9.3. Common system security parameters will be included in technical security **standards** and set appropriately on system components.

6.5.10. Full Disk Encryption

6.5.10.1. Full disk **encryption** will be deployed for operating systems containing **confidential information** (*see Endpoint Security in IS.015 Asset Management Standard* and *see IS.019 Cryptographic Management Standard*).

6.5.11. Additional Security Hardening Requirements

6.5.11.1. Reduce the attack surface presented by systems, platforms and **applications** comprising the **information system**.

6.5.11.2. Secure all resources in the Commonwealth's IT environment according to the Principle of Least Privilege.

6.5.11.3. **Information systems** that implement or connect to a directory containing non-public **information** must not permit anonymous binds.

6.5.11.4. **Information systems** that integrate with a directory used for authentication, authorization or identity **information** must connect over a secure connection.

6.5.11.5. File permissions on back-end configuration, system and **application** files must restrict access to authorized **personnel** and these files must not be accessible through the **application** or other non-administrative services.

6.5.11.6. All servers must be kept in sync with a time synchronization mechanism.

6.5.11.7. All vendor-supplied defaults must be changed to values appropriate to the environment (e.g., default passwords, SNMP permissions and community strings).

6.5.11.8. All services must run in the context of a non-privileged **user**.

6.5.11.9. Web servers must be configured to support only the HTTP methods required for **application** operation.

6.5.11.10. **Information systems** which implement HTML 5 must adhere to the HTML 5 Security Standard.

6.5.11.11. Network services must be configured to not allow low-grade TLS *encryption* and should adhere to *IS.019 Cryptographic Management Standard*.

6.5.11.12. Web servers must be configured to disallow directory listing.

6.5.11.13. Logging of detailed debugging *information* must be disabled on production systems.

6.5.11.14. Only the current non-debug-release of production code should be installed on production servers; non-production code and backup files must be removed.

6.5.11.15. Web servers must set folder permissions according to least privilege (e.g., disable unnecessary access, execute, and write permissions).

6.5.11.16. Malicious code protection must be in place.

7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18 v8	NIST CSF
6.1 Security in System and Software Lifecycle	PL-7	-	-
	PL-8	CSC 12	ID.AM-3
		-	-
	SA-1	-	
	SA-2	-	
	SA-3	CSC 4	PR.IP-2
		-	PR.IP-2
	SA-5	-	
	AU-10	-	PR.PT-1
	IA-8	CSC 6	PR.AC-1
	SC-7	CSC 4	PR.AC-5
	SC-8	CSC 3	PR.DS-2
	SC-3	-	-
	RA-3	CSC 16	ID.RA-1
6.2 Security in SDLC Support Processes	AC-3	CSC 3	PR.AC-4
	AC-6	CSC 3	PR.AC-4
	CM-2	CSC 4	
	CM-5	-	PR.IP-1
	CM-6	CSC 4	
	CM-7	CSC 2	
	CM-9	CSC 4	PR.IP-1

	MA-5	-	PR.MA-1
		-	-
		-	ID.GV-1
	CM-3	-	PR.IP-1
	CM-4	-	PR.IP-1
	SI-2	CSC 3	ID.RA-1
	IR-9	-	-
	AC-4	CSC 3	ID.AM-3
		-	PR.IP-3
	PE-19	-	PR.DS-5
6.3 System Hardening	SI-2	CSC 7	ID.RA-1
		-	DE.CM-4
	SI-4	CSC 1	ID.RA-1
		-	-
	SI-1	-	ID.GV-1
	SI-6	-	-

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting
0.95	Sean Vinck	5/7/2018	Corrections and formatting
0.97	Andrew Rudder	5/31/2018	Corrections and formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Prepublication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	NIST 800-53R5 mapping and annual review
1.4	Thomas E. McDermott	12/01/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O'Neill	12/01/2023	Final Review
1.5	Thomas E. McDermott	12/13/2024	Corrections, Formatting, Updating and Annual Review
1.5	Anthony O'Neill	12/13/2024	Final Review
1.6	Thomas E. McDermott	2/24/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	2/28/2025	Corrections and Formatting
1.6	Anthony O'Neill	3/11/2025	Final Review