Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Operations Management Standard

Document Name: Operations Management Standard	Effective Date: October 15th, 2018
Document ID: IS.023	Last Revised Date: March 11, 2025

Table of Contents

1. PURPOSE

1.1. The purpose of this ***standard*** is to document the requirements and key ***information*** security controls for ***information*** technology operations, including the definition of ***standard*** operating ***procedures***, change management, configuration management, release management, ***information*** backup and restoration and cloud computing.

2. AUTHORITY

2.1. Pursuant to 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. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

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

4.4. 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.

4.5. 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

6.1. Standard Operating Procedures

6.1.1. Commonwealth Agencies and Offices must document standard operating ***procedures*** for critical and high-***risk information systems***, to include:

6.1.1.1. Secure installation and configuration of systems.

6.1.1.2. Secure processing and handling of ***information*** (automated and manual).

6.1.1.3. Job scheduling requirements, including interdependencies with other systems.

6.1.1.4. Error and exception handling procedures.

6.1.1.5. System restart and recovery ***procedures*** to restore service in a timely manner in the event of system failure.

6.1.1.6. Logging requirements, including maintaining an audit trail for operational and security ***events***, monitoring ***procedures*** and ***log*** management ***procedures*** (*see IS.022 Logging and Event Monitoring Standard* for additional details).

6.1.1.7. Support and escalation ***procedures***, including contact ***information*** of technical support staff.

6.2. Change Management

6.2.1. Commonwealth Agencies and Offices must implement a change management ***process*** that includes:

6.2.1.1. Definition of change request categories (Critical, High, Moderate, Low, Minimal ***risk***).

6.2.1.2. Definition of the change request approval ***process***, including the level of involvement of the Change Advisory Board — High and Medium ***risk*** must be approved by the Change Advisory Board.

6.2.1.3. Identification and documentation of all change requests in a system of record.

6.2.1.4. Planning and testing of changes prior to implementation.

6.2.1.5. Verification that ***information*** security and compliance (e.g., regulatory) requirements have been met.

6.2.1.6. Identification of stakeholders and definition of communication channels to communicate change details.

6.2.1.7. Fallback ***procedures*** to recover from unsuccessful changes and unforeseen events.

6.2.1.8. Definition of the emergency change request ***process***.

6.2.1.9. Definition of a ***process*** (define the frequency of review) to perform a periodic review of the change management ***process*** to ensure compliance.

6.2.2. Emergency change requests should be regularly audited to ensure the ***process*** is being used for its intended purpose.

6.3. Configuration Management

6.3.1. Commonwealth Agencies and Offices must establish ***controls*** to maintain the integrity of ***information systems***, including:

6.3.1.1. Establish and maintain an ***asset*** inventory of authorized hardware and ***software***. Commonwealth Agencies and Offices are required to update the ***asset*** inventory on a continuing basis.

6.3.1.2. Deploy network eDiscovery tools (e.g., Tripwire IP360, NMAP, Cisco CDP) to monitor the presence of hardware and ***software*** operating within the environment.

6.3.1.3. Establish an action plan to address unauthorized or unsupported ***information systems*** on the network.

6.3.1.4. Create, maintain, and update standard operating ***procedures*** for the secure configuration of ***information systems***.

6.3.1.5. Assess compliance with configuration requirements at least annually.

6.3.1.6. Establish security hardening guideline for ***information systems,*** including commercial off-the-shelf (COTS) products. Assess compliance with security hardening requirements at least quarterly.

6.3.1.7. Deploy automated configuration management tools to track configuration settings of ***information systems*** deployed within the Commonwealth's environment (where technically feasible).

6.3.1.8. Develop action plans to address ***policy*** non-compliance or enter a ***policy*** non-compliance report.

6.3.1.9. Obtain ***Commonwealth CISO*** (or most senior security executive for ***agencies***) approval prior to implementing changes to network devices. Changes must be implemented by qualified ***personnel***.

6.3.1.10. ***Log*** and audit configuration changes to ***information systems*** and ***applications***. Changes must be consistent with details recorded in the

change request ticket.

6.3.1.11. Prohibit the use of generic and shared ***user*** IDs for configuration management activities. Change requests must be logged and monitored on a regular basis.

6.4. Capacity Management

6.4.1. Commonwealth Agencies and Offices must establish a capacity management ***process***, including:

6.4.1.1. Document a capacity management plan for mission critical systems.

6.4.1.2. Perform periodic server consolidation assessments to reduce the IT footprint.

6.4.1.3. Decommission ***applications***, databases and systems that are not required within an acceptable timeframe. ***Information systems*** that must remain operational beyond their end-of-life (e.g., vendor support life cycle) must be approved by the ***Commonwealth CISO*** (or his or her designee).

6.4.1.4. Optimize ***application*** logic, database queries, batch processing (e.g., mainframe), etc. to reduce processing power requirements and bandwidth utilization.

6.4.1.5. Deny or restrict bandwidth for resource-hungry services that are not critical for business operations (e.g., video streaming).

6.4.1.6. Rationalize disk space and remove unnecessary ***data*** that is not subject to record retention requirements.

6.5. Release Management

6.5.1. Commonwealth Agencies and Offices must document release management processes for IT environments and/or platforms.

6.5.2. Maintain separate development, test, and production environments.

6.5.3. Source code must be reviewed and tested in a lower environment prior to promotion to the production environment.

6.5.4. Production ***data*** may be used in a lower environment (non-production) under the following conditions: ***exception*** request sought and granted as specified above, and the security ***controls*** for the lower environment are consistent with the production environment.

6.5.5. Developers must not have the ability to migrate code into production environments.

6.5.6. If a dedicated release management role is not in place, Commonwealth

Agencies and Offices must ensure that ***personnel*** are issued separate accounts to perform their release management duties. Monitoring will be implemented and audited where technically feasible.

6.6. Data Backup and Restoration

6.6.1. Commonwealth Agencies and Offices must establish a ***process*** to back up ***information*** in a secure manner to enable the organization to restore its operational activities after a planned or unplanned interruption of service.

6.6.2. ***Data*** backup and retention requirements and timeframes are as follows:

6.6.2.1. Weekly: A full backup of mission-critical (from an agency, legal or regulatory perspective) ***data***.

6.6.2.2. Daily: Incremental backups.

6.6.2.3. Backup ***data*** should be retained on near-line storage for fast retrieval for the first 30 days and thereafter written to long-term secure storage per the record retention requirements.

6.6.3. The decision to back up must be reached through the use of a business impact analysis (BIA) or a ***risk*** assessment that considers, but is not limited to, the following factors:

6.6.3.1. Business need

6.6.3.2. Security requirements

6.6.3.3. Criticality of the ***information***

6.6.4. Backup and recovery must be included as part of the business continuity and disaster recovery planning.

6.6.5. Backup and recovery documentation must be reviewed, tested, and updated regularly, but not less than annually.

6.6.6. Backup records must be accurate and complete, including ***exception*** tracking (i.e., success/failures to backup). Documented restoration ***procedures*** must be maintained for ***assets*** critical to the organization.

6.6.6.1. At a minimum, ***data owner***, classification of ***data***, time of capture, retention duration and storage location must be captured.

6.6.7. Backup ***data*** must not be stored on the same media (i.e., electronic) or physical location (e.g., magnetic tapes) as the primary ***data*** source.

6.6.7.1. Backup on removable media that will be transferred or stored offsite must be ***encrypted***.

6.6.7.2. Backup on removable media must be protected from physical and

environmental hazards.

6.6.7.3. Backup on removable media must be stored in locked and secured areas. Only authorized individuals should have physical access to backup tapes. Access ***logs*** must be maintained and reviewed on a regular basis, but not less than annually.

6.6.7.4. Backup on removable media must be disposed of using secure deletion methods upon the end of life as defined in the *Physical Media Handling in IS.015 Asset Management Standard*.

6.6.8. Backup records subject to legal holds will be managed in accordance with guidance provided by EOTSS' Legal.

6.6.9. Implement ***data*** protection ***controls*** such as ***encryption*** to protect the confidentiality and integrity of backups.

6.6.9.1. For backup ***data*** that is ***encrypted*** and requires long or indefinite retention timeframes, consider ***key*** rotation in accordance with *IS.019 Cryptographic Management Standard*.

6.7. Cloud Computing

6.7.1. Commonwealth Agencies and Offices must establish standards to support the secure implementation of ***applications*** and services in public and private cloud environments.

6.7.2. The following are general requirements for all ***applications*** regardless of ***application*** tier (See *Information System Classification in IS.015 Asset Management Standard* for ***application*** tiers):

6.7.2.1. The cloud provider will provide a mechanism to track performance metrics against contractual obligations, including information on major outages and time for resolution.

6.7.2.2. Prior notification must be provided for maintenance activities, specifically, for any update, upgrade or maintenance of ***software*** or hardware equipment that may impact system performance.

6.7.2.3. Contracts must include minimum security clauses, the right to audit and relevant ***data*** protection requirements.

6.7.2.4. The cloud service provider must be able to produce ***vulnerability*** assessment reports such as SOC1/2, PCI self-assessment questionnaire (if applicable) upon request.

6.7.2.5. ***Application*** owners must be assigned for each ***application*** hosted in the cloud.

6.7.2.6. Operational policies, ***standards*** and ***procedures*** must be defined for

cloud- based ***applications***, including:

6.7.2.6.1. Access control

6.7.2.6.2. Cryptography

6.7.2.6.3. Operations security (change and configuration management)

6.7.2.6.4. Service development and maintenance

6.7.2.6.5. ***Information*** security ***incident*** management

6.7.2.6.6. Business continuity and recovery plan

6.7.2.7. Business continuity and disaster recovery plans must be documented and consistent with *IS.016 Business Continuity and Disaster Recovery Standard*.

6.7.2.8. Service level agreements, including system uptime, availability, and scalability (bandwidth, storage, and transactional volume) must be defined during the contracting phase and codified in contractual agreements.

6.7.2.9. Backup, ***data*** restoration and ***data*** retention must be consistent with the *Data Backup and Restoration* section of *IS.023 Operations Management Standard*.

6.7.2.10. ***Data*** retention and retrieval periods, including the length of time within which the Commonwealth can retrieve its ***data*** from the cloud provider post contract termination must be codified.

6.7.2.11. ***Incident*** response plans and escalation ***procedures*** must be defined for ***applications*** hosted in the cloud. Periodic metrics of security events must be provided to the Commonwealth by the cloud service provider.

6.7.2.12. ***Patch management process*** must be defined, critical security patches must be deployed consistent with *IS.010 Enterprise Vulnerability and Risk Management Policy* and *IS.025 Secure System and Software Lifecycle Management Standard*.

6.7.2.13. Access to ***applications*** must be role-based. Roles must be defined and documented. Quarterly audits of ***user*** roles must be conducted to verify appropriate separation of duties.

6.7.2.14. ***Users*** with administrative privileges must have separate ***user*** accounts for normal activities. Use of administrative accounts must be logged and periodically audited.

6.7.2.15. Generic accounts are prohibited for interactive accounts. ***Users*** must be issued individual accounts. Where technically feasible, the cloud

service provider will integrate with a Commonwealth directory service to obtain identities (e.g., Active Directory).

6.7.2.16. Password policies must be consistent with *IS.014 Access Management Standard* , any ***exceptions*** must have a documented ***exception*** approval from the ***Commonwealth CISO*** (or his or her designee).

6.7.2.17. Security reference and solution architecture diagrams must be defined for cloud-based ***applications***. ***Application*** and system dependencies and interfaces must be documented.

6.7.3. In addition to the requirements of this ***standard***, cloud ***applications*** that have a Critical-***risk*** or High-***risk*** tiering (as per *IS.015 Asset Management Standard*, Section 6.6.4) must:

6.7.3.1. Provide evidence of ***information*** security training and background checks for ***personnel*** working on cloud computing deployments supporting the Commonwealth.

6.7.3.2. Develop a contingency plan if a cloud service provider is acquired or goes out of business.

6.7.3.3. Document secure systems development and maintenance life cycle ***process***.

6.7.3.4. Define privacy and ***data*** protection requirements, including:

6.7.3.4.1. Control content replication across technology environments.

6.7.3.4.2. Control format, accuracy, and ***encryption***.

6.7.3.4.3. Control who can access content.

6.7.3.4.4. Control content life cycle and disposal.

6.7.3.4.5. ***Encrypt confidential data*** at rest.

6.7.3.4.6. ***Encrypt confidential data*** in transit.

6.7.3.5. Implement security monitoring ***controls***, including the ability to monitor and detect anomalous activity. ***Logs*** will be sent to the enterprise SIEM.

6.7.3.6. Implement intrusion detection and prevention ***controls***.

6.7.3.7. Implement forensics capabilities to assist the investigation in the case of a ***security incident*** or breach.

7. CONTROL MAPPING

Section	NIST 800-53	CIS 20	NIST CSF
6.1. Standard Operating Procedures	AU-1	-	ID.GV-1
	AU-2	CSC 6	PR.PT-1
	AU-3	CSC 6	PR.PT-1
	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	AU-8	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
	SI-11	-	-
	CP-2	-	ID.AM-5
6.2. Change Management	CM-1	-	ID.GV-1
	CM-3	CSC 3	PR.IP-1
	CM-4	CSC 3	PR.IP-1
	CM-5	CSC 3	PR.IP-1
	CM-9	CSC 3	PR.IP-1
	AC-5	CSC 5	PR.AC-4
6.3. Configuration Management	CM-1	-	ID.GV-1
	CM-3	CSC 3	PR.IP-1
	CM-4	CSC 3	PR.IP-1
	CM-5	CSC 3	PR.IP-1
	CM-7	CSC 3	PR.IP-1
	CM-8	CSC 1	ID.AM-1
	CM-9	CSC 3	PR.IP-1
	AC-5	CSC 5	PR.AC-4
	AU-1	-	ID.GV-1
	CM-2	CSC 18	PR.DS-7
	CM-6	CSC 3	PR.IP-1
	AU-2	CSC 6	PR.PT-1
	AU-3	CSC	PR.PT-

		6	1
	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	AU-8	CSC 6	PR.PT-1
	AU-11	CSC 6	PR.PT-1
	AU-12	CSC 6	PR.PT-1
6.4. Capacity Management	AU-4	-	PR.DS-4
	AU-5	CSC 6	PR.PT-1
	CP-2	-	ID.AM-5
	SA-2	-	-
	SC-5	-	PR.DS-4
6.5. Release Management	SC-32	-	-
6.6. Data Backup and Restoration	CP-9	CSC 10	PR.IP-4
6.7. Cloud Computing	AC-16	CSC 5	PR.AC-4
	AC-20	-	ID.AM-4

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections, Formatting
0.92	John Merto	01/02/2018	Corrections, Formatting
0.95	Sean Vinck	5/7/2018	Corrections, Formatting
0.96	Andrew Rudder	5/31/2018	Corrections, Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections, Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-Publication 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	Thomas E. McDermott	11/24/2023	Corrections, Formatting, Updating and Annual Review
1.3	Anthony O'Neill	11/24/2023	Final Review
1.4	Thomas E. McDermott	12/11/2024	Corrections, Formatting and Annual Review
1.4	Anthony O'Neill	12/11/2024	Final Review
1.5	Thomas E. McDermott	2/21/2025	Updates, Corrections and Formatting

1.5	Miklos Lavicska	2/26/2025	Corrections and Formatting
1.5	Anthony O'Neill	3/11/2025	Final Review