



Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Logging and Event Monitoring Standard

Document Name: Logging and Event Monitoring Standard

Effective Date: October 15th, 2018

Last Revised Date: March 19, 2025

Document ID: IS.022

Table of Contents

1. Purpose.....	2
2. Authority	2
3. Scope.....	2
4. Responsibility	3
5. Compliance.....	3
6. Standard Statements	4
7. Control Mapping	11
8. Document Change Control	11

1. PURPOSE

- 1.1. The purpose of this **standard** is to establish the minimum requirements for security monitoring and **event** management, to detect unauthorized activities on Commonwealth **information systems**. This **standard** defines the following related **controls** and acceptable practices:
 - 1.1.1. Audit requirements for **user** activities, **exceptions**, and **information** security **events**
 - 1.1.2. Logging activities and actions required to resolve system fault errors
 - 1.1.3. **Guidelines** for the frequency of reviewing audit **logs**
 - 1.1.4. Protection of audit **logs** through technical **controls** such as file permissions
 - 1.1.5. Integration of suspicious audit **events** and investigation into **incident** response **processes**

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. Logging and Monitoring

- 6.1.1. Commonwealth Agencies and Offices must ensure that a **process** to capture key security events associated with **information system** components (e.g., network devices, servers, databases) is developed and implemented to monitor system activity.
- 6.1.2. Commonwealth Agencies and Offices must make the **logs** and **events** from the monitoring system available to the Commonwealth SOC for centralized monitoring.

6.2. Audit Logging

- 6.2.1. Record **user** activities, **exceptions**, and **information** security **events**. Commonwealth Agencies and Offices will, at a minimum, record:
 - 6.2.1.1. **User** IDs
 - 6.2.1.2. Dates, times, and details of key **events**
 - 6.2.1.3. Logon success or failure indication
 - 6.2.1.4. Identity or name of affected **data**, system component, or resource and location (if possible)
 - 6.2.1.5. Records of successful and rejected **data** and other resource access attempts (e.g., **user** attempts to query databases, improper modification of **data**)
 - 6.2.1.6. Changes to critical system configuration
 - 6.2.1.7. Escalation of privileges
 - 6.2.1.8. Use of system utilities and **applications** (e.g., libsysfs, systool)
 - 6.2.1.9. Network addresses and protocols

- 6.2.1.10. Alarms raised by the access **control** system
- 6.2.1.11. Activation and deactivation of protection systems (e.g., antivirus systems and intrusion detection systems)
- 6.2.2. Audit **logs** may contain **confidential** personal **data** or **user information**. Appropriate security measures must be taken to ensure all **confidential information** is adequately protected and handled (see *IS.015 Asset Management Standard*).
- 6.2.3. Monitoring System Use
 - 6.2.3.1. Commonwealth Agencies and Offices must ensure that they have enabled audit functionality for systems and system components linked to individual **user** accounts (i.e., Commonwealth **personnel**).
 - 6.2.3.2. Commonwealth Agencies and Offices must ensure that the **Information Custodian** works with the **Information Owner** to identify required **information system** components that require monitoring system use, such as those that process, store, or transmit **confidential information** and/or are public facing (e.g., web server).
 - 6.2.3.3. Commonwealth Agencies and Offices must ensure that the **Information Owner** employs technical solutions at the network, host, **application**, and database tiers to detect anomalous activity.
 - 6.2.3.4. Intrusion-detection systems and/or intrusion prevention systems must be used to monitor traffic at the network perimeter and at critical entry points to the internal network (e.g., network segments that host **confidential information**).
- 6.2.4. System Event Monitoring
 - 6.2.4.1. Commonwealth Agencies and Offices must ensure that at a minimum, the following system **events** will be monitored:
 - 6.2.4.1.1. All authorized **user** access to **confidential information** and audit trails, including:
 - 6.2.4.1.1.1. **User** ID
 - 6.2.4.1.1.2. Date and time of key **events**
 - 6.2.4.1.1.3. Types of **events**
 - 6.2.4.1.1.4. Files accessed
 - 6.2.4.1.1.5. Program/utilities used

- 6.2.4.2. All privileged operations, including all actions taken by any individual with root or administrative privileges:
 - 6.2.4.2.1. Use of privileged accounts, e.g., supervisor, root, administrator
 - 6.2.4.2.2. System startup and stop
 - 6.2.4.2.3. System clock time change
 - 6.2.4.2.4. I/O device attachment/detachment
 - 6.1.3.2.5 Modification/flushing of **log** files
 - 6.2.4.3. Unauthorized Access Attempts:
 - 6.2.4.3.1. Failed or rejected **user** actions
 - 6.2.4.3.2. Failed or rejected actions involving **restricted** or **confidential information** or system components
 - 6.2.4.3.3. Access policy violations and notifications for network gateways and firewalls
 - 6.2.4.3.4. Alerts from proprietary intrusion detection systems
 - 6.2.4.4. System Alerts or Failures:
 - 6.2.4.4.1. Console alerts or messages
 - 6.2.4.4.2. Network management alarms
 - 6.2.4.4.3. Alarms raised by the identity and access **control** systems
 - 6.2.4.5. Changes to, or attempts to change, system security settings and **controls**, including initialization, stopping or pausing of the audit **logs**
 - 6.2.4.6. Use of and changes to identification and authentication mechanisms, including but not limited to the creation of new accounts and elevation of privileges, and all changes, additions, or deletions to accounts with root or administrative privileges
 - 6.2.4.7. Creation and deletion of system-level objects (e.g., database tables or stored procedures)
- 6.2.5. Monitoring for Information Disclosure
- 6.2.5.1. The Enterprise Security Office will monitor sources on the internet for potential **information** disclosure, and if an **information** disclosure is discovered, will notify the **Commonwealth CISO**, or his or her designee.

6.2.6. Administrator and Operator **logs**

6.2.6.1. Commonwealth Agencies and Offices must ensure that **Information Owner** activities are logged and monitored. A system managed outside of the control of **Information Owner** (e.g., system and network administrators) should be used to monitor **Information Owner** activities for compliance. **Logs** will include:

6.2.6.1.1. Time at which an **event** (success or failure) occurred

6.2.6.1.2. **Information** about the **event** (e.g., files handled) or failure (e.g., error occurred, and corrective action was taken)

6.2.6.1.3. Which account(s), and which administrator(s) and/or operator(s) were involved

6.2.6.1.4. Which system **processes** were involved (e.g., boot process, loading kernel modules)

6.2.6.2. Where possible, **Information Owner** will not have permission to erase or deactivate **logs** of systems they own

6.2.7. **Log** Review and Reporting

6.2.7.1. Commonwealth Agencies and Offices must ensure that **logs** are periodically reviewed by **personnel** from the Enterprise Security Office (or **personnel** with a security role in the **agency**) to detect anomalous **events** and apply resolutions in a timely manner.

6.2.7.2. Mechanisms will be implemented to retrieve and report **information** on the logged **events**. Commonwealth Agencies and Offices will forward **logs** to the Commonwealth SOC for ingestion into the Enterprise SIEM.

6.2.7.3. The Enterprise Security Office will use **log** harvesting, parsing and alerting tools to help facilitate the identification of **log** events that need to be reviewed, including:

6.2.7.3.1. All security **events**

6.2.7.3.2. **Logs** of all system components that store, process, or transmit **confidential information**, or that could impact the security of **confidential information**.

6.2.7.3.3. **Logs** of all critical system components

6.2.7.3.4. Enable and collect **logs** for servers and system components that perform security functions (e.g., Active Directory, firewalls,

intrusion detection systems/intrusion prevention systems (IDS/IPS) and authentication servers).

6.2.7.3.5. Where **third parties** provide and manage **information systems** for Commonwealth Agencies and Offices, contractual obligations will include requirements for capturing **log information**.

6.2.7.4. The frequency of reviews will be as follows (unless superseded by regulatory requirements):

Asset value	Log review frequency
Critical	Weekly
High	Weekly
Medium	Monthly
Low	Quarterly

6.2.7.5. Forward **logs** to a central **log** collection service or SIEM to analyze through automated **data** correlation tools.

6.2.7.6. Any interruption to the logging process (failure) must be reported to the Security Office promptly. The report should include details on the cause, expected duration, expected remediation timeline and classification of **information** impacted.

6.2.8. **Log** Protection

6.2.8.1. Commonwealth Agencies and Offices must protect **logs** from unauthorized access in accordance with legal, regulatory, and contractual obligations.

6.2.8.2. Restrict access to audit **logs** to authorized **personnel** with a specific need to know the content of the audit **logs**. The Enterprise Security Office must approve **log** access for individuals who are not preauthorized to access **logs**.

6.2.8.3. Implement **controls** to safeguard and protect the integrity of **logs**, including:

6.2.8.3.1. Limit read access of audit trails to those with a job-related need

6.2.8.3.2. Protect the audit **logs** from unauthorized modification using file-integrity monitoring tools; for in-scope PCI systems, compare **logs** for consistency at least weekly

6.2.8.3.3. Use a secure transmission protocol to send **log data** from one system to another for processing

- 6.2.8.3.4. For external-facing technologies, write **logs** to a secure internal **log** server or media device
- 6.2.8.3.5. Back up audit trails to a centralized **log** server
- 6.2.8.3.6. Use hashing or other approved forms of integrity protection to protect **logs** under legal hold
- 6.2.8.4. Prohibit disclosure of audit **logs** with **confidential information** to **third parties** unless authorized by both the **Commonwealth CISO** and EOTSS Legal. Remove **confidential information** if technically possible.
- 6.2.8.5. Retain audit trails for the required retention periods per business, legal or regulatory need. Audit **log** history must be retained for at least one (1) year, with a minimum of three (3) months immediately available for analysis.
- 6.2.8.6. Synchronize operating systems clocks for **information systems** with an approved Network Time Protocol (NTP) server or similar device.
 - 6.2.8.6.1. Critical systems have the correct and consistent time.
 - 6.2.8.6.2. Time **data** must be protected.
 - 6.2.8.6.3. Time settings must be received from industry-accepted time sources.

6.3. System Types

6.3.1. The following types of **information systems** should have logging enabled.

Category	System type
Infrastructure components	<ul style="list-style-type: none"> • Intrusion detection and intrusion prevention systems • Web proxies • Core network switches • Network routers • Network and web application firewalls • Domain Name Servers (debug logging) • Authentication servers • Domain Host Configuration Protocol (DHCP) • Web servers • Network Time Protocol (NTP) servers • Mail servers • File Transfer Protocol (FTP) servers

Service <i>applications</i>	<ul style="list-style-type: none"> • Remote access software • Virtualization management (e.g., Citrix, VMware) • Active Directory • File servers • Anti-Malware protection services • Host-based firewalls • Host-based intrusion detection • Vulnerability management software
Business <i>applications</i>	<ul style="list-style-type: none"> • Applications and enabling services (e.g., web server) • Operating systems • Databases

7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18	NIST CSF
6.1 Logging and Event Monitoring	AU-1	-	ID.GV-1
	AU-6	CSC 8	PR.PT-1
	AU-7	CSC 8	PR.PT-1
	AU-9	CSC 8	PR.PT-1
	PE-6	-	PR.AC-2
	PE-8	-	-
	SC-7	CSC 4	PR.AC-5
	SI-4	CSC 13	ID.RA-1
	AU-2	CSC 8	PR.PT-1
	AU-12	CSC 8	PR.PT-1
	SI-2	CSC 13	ID.RA-1
	AU-8	CSC 8	PR.PT-1
	AU-11	CSC 8	PR.PT-1
	AU-10	CSC 8	PR.PT-1
	AU-13	CSC 8	PR.PT-1
	AU-16	CSC 8	PR.PT-1
SA-13	-	-	

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting
0.91	John Merto	1/2/2018	Corrections and formatting
0.95	Sean Vinck	5/7/2018	Corrections and formatting
0.96	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	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	Sean M. Hughes	08/29/2022	NIST 800-53R5 Mapping and Annual Review
1.4	Thomas E. McDermott	11/30/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O'Neill	11/30/2023	Final Review
1.5	Thomas E. McDermott	12/10/2024	Corrections, Formatting and Annual Review
1.5	Anthony O'Neill	12/10/2024	Final Review
1.6	Thomas E. McDermott	2/19/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	3/5/2025	Corrections and Formatting
1.6	Anthony O'Neill	3/19/2025	Final Review