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	Effective Date: October 15th, 2018
Document ID: IS.011	Last Revised Date: November 30, 2023

Table of contents

1. PURPOSE

1.1. This ***standard*** establishes 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:

- Audit requirements for ***user*** activities, ***exceptions***, and ***information*** security ***events***
- Logging activities and actions required to resolve system fault errors
- ***Guidelines*** for the frequency of reviewing audit ***logs***
- Protection of audit ***logs*** through technical ***controls*** such as file permissions
- Integration of suspicious audit ***events*** and investigation into ***incident*** response ***processes***

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "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***, electronic and computing devices, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), such as mass.gov, must agree 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***.

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. Any inquiries or comments regarding this ***standard*** must be submitted to the Enterprise Risk Management Office by sending an email to ERM@mass.gov .

4.4. Additional ***information*** regarding this ***standard*** may be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch including 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.

Exceptions to any part of this document must be requested online through ServiceNow, https://www.mass.gov.service-now.com . A policy ***exception*** may be granted only if the benefits of the ***exception*** outweigh the increased ***risks***, as determined by the ***Commonwealth CISO***, or his or her designee. Any and all ***exceptions*** will be for a specified time and will be narrow in scope.

6. STANDARD STATEMENTS

6.1. Logging and Monitoring

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. Commonwealth Agencies and Offices must make the ***logs*** and ***events*** from the monitoring system available to the Commonwealth SOC for centralized monitoring.

6.1.1 Audit logging

Record ***user*** activities, ***exceptions,*** and ***information*** security ***events.*** Commonwealth Agencies and Offices will, at a minimum, record:

6.1.1.1. ***User*** IDs

6.1.1.2. Dates, times, and details of key ***events***

6.1.1.3. Logon success or failure indication

6.1.1.4. Identity or name of affected ***data***, system component, or resource and location (if possible)

6.1.1.5. Records of successful and rejected ***data*** and other resource access attempts (e.g., ***user*** attempts to query database, improper modification of ***data***)

6.1.1.6. Changes to critical system configuration

6.1.1.7. Escalation of privileges

6.1.1.8. Use of system utilities and ***applications*** (e.g., libsysfs, systool)

6.1.1.9. Network addresses and protocols

6.1.1.10. Alarms raised by the access ***control*** system

6.1.1.11. Activation and deactivation of protection systems (e.g., antivirus systems and intrusion detection systems)

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.004 Asset Management Standard*).

6.1.2 Monitoring system use

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***).

6.1.2.1. 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).

6.1.2.2. 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.

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***).

6.1.3 System event monitoring

Commonwealth Agencies and Offices must ensure that at a minimum, the following system ***events*** will be monitored:

6.1.3.1. All authorized ***user*** access to ***confidential information*** and audit trails, including:

6.1.3.1.1. ***User*** ID

6.1.3.1.2. Date and time of key ***events***

6.1.3.1.3. Types of ***events***

6.1.3.1.4. Files accessed

6.1.3.1.5. Program/utilities used

6.1.3.2. All privileged operations, including all actions taken by any individual with root or administrative privileges:

6.1.3.2.1. Use of privileged accounts, e.g., supervisor, root, administrator

6.1.3.2.2. System startup and stop

6.1.3.2.3. System clock time change

6.1.3.2.4. I/O device attachment/detachment

6.1.3.2.5 Modification/flushing of ***log*** files

6.1.3.3. Unauthorized access attempts:

6.1.3.3.1. Failed or rejected ***user*** actions

6.1.3.3.2. Failed or rejected actions involving restricted or ***confidential information*** or system components

6.1.3.3.3. Access policy violations and notifications for network gateways and firewalls

6.1.3.3.4. Alerts from proprietary intrusion detection systems

6.1.3.4. System alerts or failures:

6.1.3.4.1. Console alerts or messages

6.1.3.4.2. Network management alarms

6.1.3.4.3. Alarms raised by the identity and access ***control*** systems

6.1.3.5. Changes to, or attempts to change, system security settings and ***controls***, including initialization, stopping or pausing of the audit ***logs***

6.1.3.6. Use of and changes to identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges — and all changes, additions, or deletions to accounts with root or administrative privileges

6.1.3.7. Creation and deletion of system-level objects (e.g., database tables or stored procedures)

6.1.4 Monitoring for information disclosure

The Enterprise Security Office must monitor sources on the internet for potential ***information*** disclosure, and if an ***information*** disclosure is discovered, must notify the ***Commonwealth CISO***, or his or her designee.

6.1.5 Administrator and operator ***logs***

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:

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

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

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

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

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

6.1.6 ***Log*** review and reporting

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 resolution in a timely manner. 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.

6.1.6.1. 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:

6.1.6.1.1. All security ***events***

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

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

6.1.6.1.4. 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).

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

6.1.6.2. 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

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

6.1.6.4. 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.

6.1.7 ***Log*** protection

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

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

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

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

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

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

6.1.7.2.4. For external-facing technologies, write ***logs*** to a secure internal ***log*** server or media device

6.1.7.2.5. Back up audit trails to a centralized ***log*** server

6.1.7.2.6. Use hashing or other approved forms of integrity protection to protect ***logs*** under legal hold

6.1.7.3. 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.

6.1.7.4. 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.

6.1.7.5. Synchronize operating systems clocks for ***information systems*** with an approved Network Time Protocol (NTP) server or similar device.

6.1.7.5.1. Critical systems have the correct and consistent time.

6.1.7.5.2. Time ***data*** must be protected.

6.1.7.5.3. Time settings must be received from industry-accepted time sources.

6.2. System Types

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

Category	System type
Infrastructure components	• 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 ***applications***	• 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 ***applications***	• ***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. RELATED DOCUMENTS

Document	Effective date

9. 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
1.5	Anthony O'Neill	11/30/2023	Final Review

The owner of this document is the ***Commonwealth CISO*** (or his or her designee). It is the responsibility of the ***document owner*** to maintain, update and communicate the content of this document. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

9.1 Annual Review

This document, the *Logging and Event* Monitoring *Standard*, should be reviewed and updated by the ***document owner*** on an annual basis or when significant ***policy*** or ***procedure*** changes necessitate an amendment.