Security Logging and Event Monitoring Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
March 31, 2026

Supersedes:
ITP-SEC021

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

The purpose of this Information Technology Policy (ITP) is to provide the requirements for security logging and event monitoring.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

4.1 Security Information & Event Manager Solutions

Agencies that desire to leverage the Enterprise SIEM should contact the Enterprise Information Security Office (EISO) at ra-ciso@pa.gov to gain access.

Agencies that have a SIEM solution or that are looking to procure a new SIEM solution must comply with the standards as outlined below and in the *Security Logging and Event Monitoring Standard.*

In addition, some agencies may be subject to additional requirements due to federal laws, statues, or regulations (e.g., HIPAA, IRS Publication 1075, CJIS Security Policy, PCI, etc.). Agencies should be aware and ensure compliance with any additional requirements not explicitly outlined in this policy.

4.2 Logging Requirements

Agencies shall develop and implement a process to capture system activity on key Events associated with Commonwealth IT Resources. Refer to the *Security Logging and Event Monitoring Standard* for further policy guidance on the types of Logs and Events to be captured.

Logs and Events from the monitoring system shall be made available to the EISO for centralized monitoring when technically feasible.

4.2.1 Administrator Logs

Agencies shall ensure that activities performed by an administrator are logged and monitored in a system managed outside of the control of the administrator. Refer to the *Security Logging and Event Monitoring Standard* on logging requirements for administrators.

4.2.2 Logging and Monitoring of System Use

Agencies shall:

- Enable audit functionality for systems and system components linked to individual user accounts.
- Identify the Commonwealth IT Resources that require monitoring such as, but not limited to, those that process, store, or transmit Class "C" or Closed Records per the *Data Classification Policy* and/or are public facing.
- Employ technical solutions at the network, host, application, and database tiers to detect anomalous activity.

4.3 Monitoring Requirements

The EISO is responsible for the monitoring of the enterprise SIEM solution. If a SIEM solution is deployed within an agency, the responsibility is that of the agency to ensure all monitoring requirements as outlined in the *Security Logging and Event Monitoring Standard* are met in accordance with policy.

4.4 Log Protection

Agencies must protect Logs from unauthorized access and in accordance with Commonwealth policy, legal, regulatory, and contractual obligations. Refer to the *Security Logging and Event Monitoring Standard* for a listing of measures that shall be implemented to aid in this protection.

4.5 System Types

Agencies shall ensure that all system types identified in *Security Logging and Event Monitoring Standard* have logging enabled.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy

exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document