Information Technology Policy

Security Logging and Event Monitoring Policy

Number
ITP-SEC021

Effective Date
October 10, 2006

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
March 2025

1. Purpose

The purpose of this Information Technology Policy (ITP) is to provide the requirements for security logging and event monitoring to detect and/or identify potential security incidents, policy violations, operational concerns, and unauthorized or fraudulent activities on Commonwealth IT Resources. In addition, the Logs and/or Events generated can be utilized when performing audits, forensic analysis, internal investigations, establishing baselines and identifying trends or problems.

2. Scope

This ITP 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 ITP as outlined in the Responsibilities section.

3. Definitions

Event(s): Any observable occurrence in a network or system.

Log(s): A record of the Events occurring within a network or system.

Security Information & Event Manager (SIEM): An application that provides the ability to gather security data from information system components and present the data as actionable information via a single interface.

4. Policy

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 *STD-SEC021A, Security Logging & Event Management Standards (Commonwealth Access Only).*

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 STD-SEC021A 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 STD-SEC021A 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 *ITP-INF015 Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* 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 STD-SEC021A 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 STD-SEC021A 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 STD-SEC021A have logging enabled.

5. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

5.3 Third-party vendors, licensors, contractors, or suppliers shall:

Log Events including: log collection and consolidation, security event collection from multiple sources (firewalls, routers, servers, etc.), identification of security related events and incidents, automated response/alerting capability when incidents are detected, and correlation of events from multiple sources.

6. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx
- *Management Directive 205.34 Amended Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Manual 210.09 Amended, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*
- *STD-SEC021A, Security Information and Event Management Standards (Commonwealth Access Only)*
- *ITP-INF015, Policy & Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*

- *ITP-SEC031, Encryption Standards*
- *NIST 800-92, Guide to Computer Security Log Management*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver must be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	10/20/2006	Base Document	N/A
Revision	05/9/2013	Updated the policy to reflect current standards making it easier for agencies to implement SIEM solutions. Rescinds STD-SEC021A and incorporates elements of OPD-SEC021B.	N/A
Revision	04/2/2014	ITP Reformat	N/A
Revision	03/04/2024	ITP Reformat Updated Title Updated Purpose. Updated Scope based on connection to Commonwealth Network and added language for 3rd party vendor applicability. Added definitions for events, logs, and SIEM. Created section headings with Policy section. Added language under Section 4.1 regarding additional requirements/regulations some agencies may have. Added Section 4.2 Logging Requirements and accompanying policy language including subsections 4.2.2. Administrator Logs and 4.2.3 Logging and Monitoring of System Use. Added Section 4.3 Monitoring Requirements Added Section 4.4 Log Protection Added Section 4.5 System Types Updated references.	Revised IT Policy Redline <03/04/2024>