P.17

Policy Name

Security Operations Policy

1. Purpose

This Policy establishes the foundation for effective security operations, including the consistent logging of enterprise information systems, the compiling of log data, and the capacity to analyze and search the data for anomalous behavior and other indicators of threats.

2. Scope

The Statewide IT Policies and Standards ("POLICIES") apply to all IOT-supported entities ("Entities"), their employees, their contractors, their consultants, and their vendors Unless otherwise specified, all of the POLICIES apply equally to physical and electronic assets and resources assigned to an individual, on-premises physical assets, on-premises virtual assets, on-premises cloud assets, assets provided by cloud service providers, products and/or services that use cloud computing, all data stored or processed by the above assets in electronic, paper, or any other form, and everything else that supports the functioning of State government ("State Enterprise").

3. Policy

IOT must deploy a security information and event management ("SIEM") tool for collecting, compiling, and analyzing State Enterprise log data it considers valuable for the functions identified in this Policy.

3.1. Threat Intelligence

a. IOT must maintain subscriptions to available threat intelligence services and have mechanisms in place for tracking internal and external sources of threat information.
b. IOT should have access to established sources of threat intelligence with a review process to confirm the efficacy of the sources.
c. Threat intelligence teams should share intelligence to provide for the improved detection of threats.
d. Threat intelligence teams should share indicators of compromise ("IOCs") to support security operations center ("SOC") analysts with their triage of alerts.

3.2. System Logging

a. Entities must configure systems to transmit security and audit logs to IOT's SIEM in accordance with the Security Logging Standard.
b. If an Entity maintains its own SIEM, it must configure systems to transmit security and audit logs to its own SIEM in accordance with the Security Logging Standard.
c. IOT should have a process in place to ensure that logging is enabled on information systems deemed critical.
d. IOT must have a standard time stamp for audit records, and a system that compares and synchronizes internal system clocks with an authoritative source for audit records.
e. Logging and monitoring systems must protect audit logging information and audit logging tools from unauthorized access, modification, and deletion in accordance with defined data protection and retention requirements.

3.3. Log Aggregation, Alerts, and Identification of Subjects for Incident Response

a. IOT must maintain the ability to review and search log data compiled from various information systems.
b. IOT and Entities must ensure adequate system capacity to meet data retention requirements.
c. IOT and Entities must establish business continuity and disaster recovery resources and processes for the continuity of threat intelligence.
d. Entities must notify IOT of federal, state, or other obligations regarding log retention.
e. IOT must establish a process for triaging alerts and identifying subjects for incident response.

4. Exceptions

Exception Requests will be addressed through the process designated by IOT.

5. Ultimate Authority

The Chief Information Officer is the ultimate authority for decisions made pursuant to the POLICIES, including Exception Requests.

6. Roles and Responsibilities

State agencies vary tremendously. Some State agencies have Chief Information Officers, while others may have no dedicated IT employees. Because of that variance, the Statewide IT Policies and Standards do not refer to a specific job title as being responsible for compliance. Instead, the intent is for the responsibilities to rest with the agency head or the highest-ranking employee responsible for IT, unless stated otherwise regarding a specific duty.

7. Statutory Purposes

The statutory purposes of IOT include "establish the standards for the technology infrastructure of the state" and "provide for the technology and procedures for the state to do business with the greatest security possible," Ind. Code § 4-13.1-2-1(1) and (5). IOT has an obligation to "develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government," Ind. Code § 4-13.1-2-2(a)(11).

8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.