P.18

Policy Name

Security Tools Policy

1. Purpose

This Policy establishes the requirements for tools used to maintain and secure the State Enterprise.

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

3.1 Security Tool Requirements

a. IOT must select, maintain, and regularly review security tools.
b. IOT must deploy a standard set of security tools on end user devices and server infrastructure.
c. Endpoint detection tools must be broadly deployed across state assets.
d. Vulnerability management is as relevant with security tools as with any other information resource. See the Vulnerability Management Policy.

3.2 Endpoint Security Requirements

a. IOT will build and maintain systems from a standard configuration baseline, including cybersecurity hardening requirements.
b. For an endpoint device capable of running an antivirus software program, IOT and Entities must subscribe the endpoint device to the state antivirus service, with connectivity to support periodic virus signature file updates.
c. For an endpoint device capable of running a host-based threat detection and response software program, IOT and Entities must subscribe the endpoint device to the enterprise endpoint detection and response ("EDR") service, with connectivity to support periodic detection logic or rule updates.
d. Disabling or removing antivirus or EDR software, or disabling software updates to antivirus or EDR, is prohibited.

3.3 Application Security Requirements

a. Applications must be periodically scanned to identify application layer vulnerabilities. This includes dynamic scans of the functioning application, and static scans of the underlying source code and compiled binaries.
b. Vulnerabilities must be remediated according to defined timelines, based on the criticality.
c. Critical applications must be subscribed to the application security testing services, with connectivity to the central console to support periodic reporting.
d. Disabling application security testing services is prohibited.

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.