P.21

Policy Name

Vulnerability and Patch Management Policy

1. Purpose

The purpose of this Policy is to establish the requirements for identifying and remediating vulnerabilities within the State Enterprise. This Policy also provides obligations for the Patching of tools and applications.

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 Identification and Discovery

a. IOT and Entities must implement and maintain a program to assess and track vulnerabilities on IT assets within the State Enterprise.
b. The vulnerability management program will incorporate the most currently available asset management data to refresh the scope of Scans.
c. Regular penetration tests must be conducted to support the identification of potential vulnerabilities.
d. The program should also provide for a recurring feedback loop between vulnerability Scanning, Patch management, and configuration management processes to monitor for the remediation of identified vulnerabilities.
e. IOT must gather and analyze information on negative security events experienced by other organizations.
f. IOT may share information with Entities potentially impacted by identified vulnerabilities. At the discretion of the Chief Information Officer, IOT may share information on threats and vulnerabilities with external parties.

3.2 Vulnerability Scanning

a. IOT must use vulnerability-Scanning technologies ("Scan" or "Scanning") as a primary vulnerability management discovery mechanism.
b. IOT must Scan to identify the presence of vulnerabilities within operating systems, databases, some workstation applications, network resources, and other information resources owned or managed by IOT, such as cloud or Software-as-a-Service ("SaaS") applications.
c. IOT must Scan the following information resources at least monthly:
    i. All physical and virtual servers supported by IOT
    ii. All workstations supported by IOT
    iii. All network equipment supported by IOT
    iv. Internally developed applications (See the Development and SDLC Policy.)
    v. Commercial and proprietary cloud and SaaS application
d. An Entity or its vendor must Scan monthly to identify the presence of vulnerabilities within all applications that the Entity manages.
e. Entities, their employees, their contractors, and their vendors are prohibited from blocking the functionality of a Scanning technology.
f. Based upon information gathered through Scanning and information gathered on vulnerabilities exploited by other organizations, IOT and an Entity must determine whether to perform a remedial activity, the urgency for performing the remedial activity, and how to perform the remedial activity.

3.3 Patching

a. For an application managed by an Entity, the Entity must deploy a Patch ("Patch" or "Patching") provided by the manufacturer of the respective application. IOT must deploy other Patches.
b. Zero-day vulnerabilities with identified exploits must be prioritized and remediated within the required due date.
c. IOT may deploy a Patch without an Entity's prior authorization if the information resource is two or more Patches behind the manufacturer's most recently released Patch.
d. For all newly discovered vulnerabilities, Patch deployment should align with the chart below:

Severity Level	Severity Description	Remediation Service Level
Critical	Vulnerabilities with a CVSS score of 9.0 or higher and can be readily exploited or compromised with publicly available malware exploits.	Within 15 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps. Sooner if feasible.
High	Vulnerabilities with a CVSS score of 7.0 to 8.9 with no known publicly available malware exploit.	Within 30 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.
Medium	Vulnerabilities with a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	Within 90 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.
Low	Vulnerabilities with a CVSS score of 0.0 to 3.9. Not all low-severity vulnerabilities can be easily mitigated due to application, operating system, and/or business requirements.	Within 120 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.

3.4 Validation, Testing, and Reporting

a. An Entity must test either (1) before deploying the Patch or other remediation within a non-production environment that is functionally identical to its production environment, or (2) after deploying the Patch or other remediation and at least eight hours before the next business day.
b. IOT must Scan information resources to determine whether a remedial activity was performed correctly. An Entity or its vendor must Scan an application to determine whether a remedial activity was performed correctly.
c. IOT will provide Entities with updated vulnerability metrics on a monthly basis.

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.