P.19

Policy Name

Software Development Policy

1. Purpose

The purpose of this Policy is to ensure security and due diligence in the development of software.

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. SDLC General Requirements and Environment

a. IOT and Entities that perform software development must establish and maintain a secure application development process ("software development life cycle" or "SDLC").
b. IOT must implement architecture designs, software development techniques, and system engineering principles that promote effective security within all information systems and assets. This should include referencing industry standards and leading practices.
c. IOT and Entities must protect data, pursuant to the Data Classification Policy and Standards.
d. IOT and Entities must logically separate development and testing environments from the production environment.
e. Separation of duties between development team members must be implemented, including the separation of roles between development personnel and those with the ability to push code into production.
f. Cybersecurity development techniques must be implemented following the SDLC to ensure that contractors, State-employed developers, and engineers are following the same unified process.
g. Developers should undergo specialized security training to enhance fundamental security skills.

3.2. Planning and Development

a. Roles must be identified to ensure that responsibilities for cybersecurity and privacy are established prior to development.
b. Security design principles, as well as privacy by design, should be established to ensure that relevant laws, regulations, and standards are considered during the software development process.
c. IOT may designate security requirements for the SDLC. In performing software development, individuals must consider industry standards and may incorporate threat modeling.
d. Common application vulnerabilities must be considered when planning development. Where possible, developers should use code-level security checks, such as static application security testing ("SAST"), to identify potential flaws.
e. Build and release pipelines must be managed by the assigned development teams.
f. Quality assurance testing must be performed by development teams to ensure that functionality is maintained and that all security controls are in place.
g. Developers must not be granted local administrative access. Developers must work with system administrators to acquire software releases from manufacturers.

3.3. Validation and Monitoring

a. Vulnerability scanning is required on applications before being released into production.

b. Penetration testing may be required, depending on regulatory and application requirements and criticality.
c. IOT should define a systematic process to prioritize and triage identified security vulnerabilities, along with an acceptable level of risk for system releases. A release that exceeds a defined criticality may require an Exception.
d. Developers and engineers are responsible for root-cause analysis and correcting vulnerabilities.
    i. Vulnerabilities that have not been remediated must be tracked until they are closed.
    ii. Final testing of remediated vulnerabilities should be performed to validate that all issues have been resolved, and functionality is maintained.
e. Future maintenance must follow the SDLC to maintain security controls and prevent new vulnerabilities.
f. Post validation checks must follow the implementation process, where appropriate.

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.