P.10

Policy Name

Governance and Risk Management Policy

1. Purpose

The purpose of this Policy is to support information security governance and risk management for the State's network, data, and information systems. Information security risk management is the process of identifying and prioritizing threats to the 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

IOT will operate an information security risk management function to evaluate, monitor, and prioritize risks to the State's information systems.

3.1 Program Elements

a. IOT must implement procedures and guidelines for identifying, analyzing, and monitoring information security risks.
b. IOT must use framework-based measurements for assessing and quantifying information security risks and their potential impact to the organization.
c. IOT must have a process in place for risk acceptance, including consideration of Exception Requests.

3.2 Risk Identification

a. IOT must develop and implement a process for identifying and reviewing new and emerging information security risks. This process should use internal data, as well as external threat feeds where available.
b. IOT should conduct an annual review of information security risk.
c. IOT and Entities should notify the IOT GRC and Resiliency Services team of any new or emerging information security risks.

3.3 Risk Analysis and Prioritization

a. IOT should implement a best-practice method or tool for quantifying and measuring risk.
b. IOT and Entities should conduct risk assessments, especially of critical information systems.
c. Risk assessments may be conducted by IOT or a third party.

3.4 Risk Response and Treatment

a. IOT must have documented processes in place for responding to information security risks.
b. Entities should have documented processes in place for responding to information security risks.
c. IOT and Entities may respond to a risk by using one or more of the following methods:
    i. Avoid: Eliminate, withdraw from, or omit to engage in an activity creating risk
    ii. Transfer/Share: Transfer responsibility for the risk through processes such as, but not limited to, insurance
    iii. Reduce/Mitigate: Control the risk through additional or optimized controls
    iv. Accept: Accept the risk and plan for the expected impact

3.5 Monitoring and Management

a. IOT must collect and document mitigating activities associated with information security risks and establish a cadenced review.
b. IOT should produce a cybersecurity risk report quarterly, providing an update on information security risk trends, new or modified risks, and mitigation activity progress.

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.