P.20

Policy Name

Third-Party Risk Management Policy

1. Purpose

The purpose of this Policy is to establish requirements for third-party performance, accountability, and relationships with third parties.

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 Third-Party Risk Management

a. A "Third Party" means a vendor, service provider, contractor, consultant or any other organization considered for such status, with at least one of the following:
    i. Access to the State network, or
    ii. Impacts on the State network.
b. IOT and Entities are responsible for managing activities conducted by third parties, identifying and controlling the risks arising from such relationships, and ensuring that compliance with applicable regulations has been achieved.
c. IOT and Entities should assess, measure, monitor, and control risks associated with the use of a Third Party. This includes reputational, operational, financial, compliance, and cyber risks.
    i. Planning
        - IOT must maintain a Third-Party Risk Management Policy and Standard.
        - Entities are responsible for ensuring compliance with the policy and standard.
        - IOT and Entities must maintain an inventory of all third parties.
    ii. Due Diligence
        - IOT and Entities should perform due diligence to assess the risks associated with the potential use of a Third Party, including whether the Third Party is suspended, debarred, or otherwise excluded from contracting with the federal government or the State of Indiana.
        - After engaging a Third Party, IOT and Entities should perform cadenced reviews of the Third Party, its performance, the risks resulting from the relationship with the Third Party, and whether it has been suspended, debarred, or otherwise excluded from entering relationships with the federal government or the State of Indiana.
    iii. Contracting
        - IOT and Entities must define and use standard contract language in agreements with all third parties.
        - The standard contract language must include cybersecurity and IT requirements, and requirements for data management, at the conclusion of the relationship with the Third Party.

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.