P.09

Policy Name

Exceptions Management Policy

1. Purpose

The purpose of this Policy is to establish the process and conditions for accepting the risk created by noncompliance with the Statewide IT Policies and Standards. This Policy defines the requirements for tracking Exceptions through request, approval, continuous monitoring, and review. These requirements are designed to ensure compliance with all Statewide IT Policies and Standards unless there is an authorized business justification. This Policy also underscores the importance of proactive risk identification, planning for mitigation, and appropriate resource allocation for achieving mitigation.

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

An Entity may submit a written Exception Request to IOT. IOT will document the Exception in the State's Governance, Risk, and Compliance ("GRC") tool.

3.1 Request Management

a. The Requesting Entity must submit an Exception Request within the in the State's GRC tool.
b. Requests for Exceptions must follow the required fields within the GRC platform and be authorized by a designated State employee prior to submission. Further, the Request must document:
    i. The Policy or Standard for which the Exception is needed
    ii. The provision or sentence within the Policy or Standard for which the Exception is needed
    iii. The business justification and impact, including precise details
    iv. The identified risks
    v. The compensating controls that are planned or implemented to reduce the additional risks to a tolerable level
    vi. A remedial plan, including the planned deployment date for achieving remediation, whether remediation can be achieved with existing resources, and what additional resources would be required for achieving remediation
    vii. IOT may use information from Exception Requests to inform its enterprise Risk Register.
c. An Exception Request may address only a period of six months. If the noncompliance persists, the Entity must submit a new Exception Request with the updated information, including updates on the plan for remediation.
d. If the original Exception conditions have substantially changed, a new Exception Request must be submitted.

3.2 Acknowledgement

a. IOT must review Exception Requests. The Chief Information Security Officer or their appointed designee may acknowledge, deny, or seek additional information for Exception Requests.
b. All Exceptions must be reviewed.
c. Automatic renewal is not permitted.
d. If the remediation of an Exception is deployed, the Exception must remain in place until the solution or change is reviewed and fully implemented.

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.