State of Indiana Policy and Standards

Security Policy Overview

Standard ID
IOT-CS-SEC-005

Published Date
9/1/2016

Effective Date
9/1/2016

Last Updated
9/1/2016

Next Review Date
9/1/2017

Policy
00.0 Introduction
00.1 Overview of Security Policies

Purpose
Provide an overview of the State of Indiana's Information Security Policy and an introduction to its format and structure

Scope
IOT Supported Entities

Statement
IOT is responsible for developing and maintaining comprehensive policies and standards that are predicated on the following principles:

- To ensure **confidentiality, integrity and availability** of sensitive information
- To provide for the **protection** of proprietary mission-critical information resources
- To ensure management and employee **accountability** for information resources including assets and information entrusted to them
- To ensure **compliance** with legal and regulatory requirements
- To minimize **risk** to the State's information resources

The Chief Information Security Officer (CISO) shall develop information security policy and standards, the Chief Technology Officer (CTO) shall develop architectural policy and standards, the Chief Operational Officer (COO) and the Chief Administrative Officer (CAO) shall develop Operational and Technology Policies and Standards. Policies and standards shall serve as a minimum baseline for executive branch agencies and shall be regularly reviewed and updated to properly reflect changing risk conditions and mitigation opportunities. Agencies shall develop additional or more constraining policies as required.

The State's structure of Policy is represented by four categories:
Policy - high-level statements that reflect organizational goals/objectives
Control Standard/Standard - mid-level statements that formally define controls/requirements.
Guideline - Mid-level statements that are recommended but not required
Procedure - The most granular and low-level statements which provide step by step instructions for performing a certain process, implementation, etc.

Security Policies align to the Categories described in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and both Area and Sections align to the Subcategories described in the NIST CSF.

Control Standards are the core of the policy structure and are aligned with NIST Special Publication (SP) 800-53 Revision 4 controls. Further, control standards follow a hierarchical approach and have multiple types. A hierarchy is required as agencies may wish to implement standards that are more stringent than the State's requirements, set by IOT.

Hierarchy:

Tier 1 - Control Standards written by IOT for the enterprise, all agencies are required to demonstrate compliance and file exceptions (when allowed) against Control Standards
Tier 2 - Control Standards written by agencies that meet or enhance Control Standards written at the Tier 1 level, or cover an area that is not represented in the State body of Policy.

Types – There are multiple types of Control Standards that can be written, below are the four defined in the State environment:

1.Architectural – established by IOT architects as required configurations (e.g., how applications must be configured for the PZ)

2.Operational – established by IOT service delivery teams as requirements for day-to-day items (e.g., email retention)

3.Security – established by the IOT security team as requirements for controls related to identifying, protecting, detecting, responding and recovering from information security related items

4.Technology – established by IOT service delivery teams as requirements for standardized technology (e.g., available laptop choices)

Roles

Agency Personnel

IOT Personnel

Responsibilities

IOT Security shall update State Policy and Standards based on best practices that best meet the State's requirements. Agencies shall evaluate their requirements and develop Tier 2 Control Standards, as necessary.

Management Commitment

Management shall periodically review the format and structure of State Policy and make changes that best fit the State's objectives.

Coordination Among Organizational Entities

IOT shall make State Policy and Standards available to all Executive Branch agencies under the scope of the body of policy.

Compliance

Management shall periodically review the format and structure of State Policy and make changes that best fit the State's objectives.

Exceptions

No exceptions.

Associated Documents

Policy Management