P.06

Policy Name

Data Classification and Management Policy

1. Purpose

The purpose of this Policy is to establish a comprehensive framework for categorizing and safeguarding data, including for purposes of cybersecurity and regulatory compliance.

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. Data Inventory, Data Flows, and General Protection Requirements

a. IOT must establish and maintain a data inventory that includes all sensitive data.
b. The data inventory must be reviewed and updated annually or when significant changes occur.
c. IOT and Entities must create data flow documentation for all systems, applications, and processes that involve the handling of sensitive data. These should be reviewed at least annually.
d. All individuals with access to, or who have responsibility for handling, data are required to undergo training in data protection and management.
e. IOT and Entities should implement processes that include data protection by design. "Data protection by design" refers to the integration of data protection considerations into the design and development of systems, processes, and services.

3.2. Data Retention and Disposal

a. IOT and Entities must limit the storage of data to that which is required for business, legal, and/or regulatory purposes. See Data Retention Standard.
b. Where possible, IOT and Entities should reduce the amount of data stored.
c. IOT and Entities must ensure that data disposal is conducted in accordance with a defined data retention schedule.

3.3. Data Classification

a. IOT should establish a Data Classification Standard including categories such as sensitive, confidential, and public.
b. Data classification categories must be reviewed and updated annually or when significant changes occur.

3.4 Data Loss Prevention

a. IOT must implement data loss prevention ("DLP") tools to identify all sensitive data stored, processed, or transmitted in the State Enterprise.
b. IOT and Entities should develop an inventory of sensitive data to be reviewed and updated annually, and/or upon significant change to the environment.

4. Exceptions

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.