P.03

Policy Name

Asset Management Policy

1. Purpose

The purpose of this Policy is to define the requirements for managing hardware, software, and third-party cloud applications. This Policy also provides a framework for IOT-supported entities to perform Asset management services supplemental to those provided by IOT.

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 Definitions

a. "Asset" means hardware, software, firmware, cloud resources, or any other tool deployed to support the State's information systems.
b. "Asset Inventory" means the inventory identified by IOT.
c. "Hardware" means a type of Asset that includes servers, data center resources, workstations, and other endpoints.
d. "Owner" means the person responsible for the Asset.

3.2 General Provisions and Asset Lifecycle Management

a. An Entity must neither procure nor deploy an Asset other than one authorized by IOT.
b. Upon a person's termination of state service, three-month leave, or transfer to a different Entity, an Entity must return to IOT all Assets assigned to that person, including all workstations, cell phones, tablets, identification badges, and any other tools used for identification, access, or encryption.
c. IOT must reimage an Asset before reissuing it.
d. The Asset lifecycle includes, but is not limited to, each of the following:
    i. Acquisition
    ii. Receipt
    iii. Deployment
    iv. Maintenance
    v. Physical and virtual location
    vi. Destruction
e. Where applicable, the lifecycle will also include:
    i. The person to whom the Asset is assigned
    ii. Contact information for the assigned person
f. IOT and Entities must maintain accurate and updated information regarding Assets in the Asset Inventory and throughout the Asset lifecycle. IOT and Entities must annually review and update this information.
    i. The Asset Inventory should integrate information from several information systems, including procurement, billing, shipping, configuration, and destruction.
    ii. IOT will configure the Asset Inventory to require certain information, which will vary depending on the type of Asset. The Asset Inventory should include the Asset's Owner, details on its connection to the network, and its criticality.

3.3 Hardware

a. All Hardware above $500 in value must have an Owner.
b. Hardware must have a mechanism for identification to enable accurate tracking and management. This may be implemented through Asset tags.
c. All new Hardware must be approved and reviewed before it can be allowed on the network.
d. IOT will provide tools for identifying, scanning, patching, updating, and logging Assets, and centrally managing Asset control.
    i. An Entity must ensure that its Assets are powered and connected to the State of Indiana network or to internet service at least every three months.
    ii. Neither an Entity nor a person may disable a tool deployed for any of the above-named purposes.
e. IOT and Entities will designate approved individuals to ship Assets to office spaces and other facilities used for State of Indiana business. Shipping Assets to a residence is prohibited.
f. Owners are responsible for ensuring that all assigned Assets remain within vendor support. When seeking extended support, an Entity must use the IOT-approved extended support vendors.
g. IOT and Entities must maintain a warranty on all servers. Procuring an extended warranty is required when an Asset is no longer covered by the initial plan.
h. IOT will assign a unique identifier to each hard drive and maintain proof of destruction for all drives. IOT will enforce the sanitization of cloud-hosted data through the use of contractual language and verification processes, depending on the specific cloud vendor.
i. IOT will manage the process by which workstations are refreshed and upgraded.
j. The Asset Inventory should provide categorizations based on the business use and the environment in which the Hardware will be used. Categorizations must allow for the prioritization of Assets.
k. Assets must be destroyed using IOT's approved methods. The destruction of an Asset requires a ticket documenting the Asset's destruction.
l. IOT should perform periodic scanning for rogue wireless access points.
m. Appropriate diagrams depicting relevant electronic communications and data flows between Assets must be maintained and reviewed by IOT for accuracy at least annually, or upon significant changes to the environment.

3.4 Software, External, and Cloud Assets

a. All software and cloud Assets must have an Owner.
b. Software and cloud Asset inventories must be reviewed at a defined interval to ensure that listings are accurate, and licensing is up to date. Inventories should include a categorization based on business use and the environment in which the software or cloud Asset is used.

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.