P.13

Policy Name

Maintenance Policy

1. Purpose

The purpose of this Policy is to establish requirements for the logging, tracking, and managing of maintenance performed on the State Enterprise, including on-site and remote maintenance.

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 Operational Maintenance

a. IOT and Entities must specify the individuals authorized to perform maintenance.
b. A vendor to IOT or another Entity must submit to IOT a written description of its operational maintenance procedures within 30 calendar days of IOT's written request. This obligation applies regardless of whether the vendor's maintenance is performed by the vendor itself or a different organization.
c. IOT and Entities must establish procedures to ensure appropriate oversight of all maintenance activities on the systems they manage.
d. IOT and Entities must maintain the following maintenance records:
    i. Date and time the maintenance was performed
    ii. Names of staff performing maintenance
    iii. Name of the person who authorized the maintenance
    iv. Description of the maintenance performed
    v. List of replaced components
e. Any component removed from the system must be sanitized, pursuant to the U.S. National Institute of Standards and Technology ("NIST") Special Publication 800-53 Rev.5.
f. Maintenance tools must be inspected for malicious code as part of the authorization process. Approved tools must be documented. An individual performing maintenance must be trained on the tools available for use.
g. IOT and Entities must monitor maintenance activities and limit the time period in which maintenance may be performed.
h. Maintenance activities must follow IOT's change management process.
i. IOT and Entities must maintain warranties on servers. See the Asset Management Policy.

3.2 Entity Responsibilities

An Entity must establish and implement IT security procedures, including training, for the secure operation and maintenance of remote devices that fall outside of IOT's management.

a. Device operating systems must be maintained with appropriate vendor security patches and updates.
b. Mandatory system configurations, settings, and software for state-owned devices must not be modified without prior authorization by IOT.
c. Entities must develop guidelines on the management and maintenance of data.

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.