P.16

Policy Name

Security Awareness and Training Policy

1. Purpose

The purpose of this Policy is to establish the requirements for a security awareness program.

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. Security Awareness and Training Administration

a. IOT must establish and maintain a security awareness program and provide training to Entities.
b. Users must complete any assigned security training.
c. IOT must establish and maintain a security awareness training platform to support hands-on phishing simulations. Phishing training should be of varying complexity to mirror current, active attack patterns.
d. The delivery mechanism will be through an online site or through the State's learning management system.

3.2 General Training and Awareness Requirements

a. The training is periodic in nature, as often as monthly. Users are required to complete assigned training within the specified time.
b. IOT will review and update the training content annually, or as needed, based upon the current, active threat patterns.
c. The following provides an example of a general set of items that are covered directly or indirectly as part of the overall training and awareness program:
    i. Email Security/Phishing
    ii. Information Protection
    iii. Passwords and Authentication Best Practices
    iv. Physical Security
    v. Social Engineering

3.3 Specialized and Role-Based Training

a. Entities should review opportunities to incorporate relevant role-based security training into their workforce (e.g., security-sensitive positions, executive leadership, privileged users, incident response).
b. Entities should train employees involved in managing sensitive data on data management and security practices related to their specific roles. This is especially true regarding data protected by law and data received from a Federal agency, such as Protected Health Information ("PHI"), Federal Tax Information ("FTI"), and Criminal Justice Information Services ("CJIS") information.
c. IOT and Entities must use supplemental opportunities for enhancing security awareness through newsletters, awareness months, office visuals, and other communication mechanisms, where applicable.

3.4 Reporting and Remediation

a. Reporting will be provided to Agency management for completion rates, including specific users that have not completed a training.
b. Remediation training may be provided to users who fail specific training exercises, such as phishing simulations.
c. IOT may implement protective measures for a user that has not completed training.

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.