Data Technology Authority (ITA)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4505 – Cybersecurity Awareness Training

CONTENTS:

I. Authority
II. Abstract
III. Policy
IV. Exemption Process
V. Procedure Reference
VI. Contact Data
Revision History

I. AUTHORITY

Authority: Idaho Code § 67-833

II. ABSTRACT

Awareness and training are key elements of a successful cybersecurity program.

The goal of awareness is to focus attention on cybersecurity, increase recognition of the need to protect data, and increase users' understanding of risks associated with threats and vulnerabilities.

The goal of training is to build the knowledge and skills needed to facilitate individual job performance. Cybersecurity training is essential for the people who operate and support existing systems, design and deploy new systems, or require advanced specialty skills (such as digital forensics).

III. POLICY

A. The State of Idaho's mandatory cybersecurity awareness training shall ensure all system users are provided basic information system cybersecurity awareness guidance upon authorizing access to the system and at least annually thereafter.
B. The State of Idaho shall perform a gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to focus a training and awareness roadmap for all employees.
C. The State of Idaho shall document, validate, and improve cybersecurity awareness levels and training through periodic tests and evaluations. Targeted

training should be provided to those who fall below established minimum thresholds.

D. Each agency shall identify and implement supplemental cybersecurity training based upon their agency's unique requirements. This may be in the form of supplemental training using the State-identified cybersecurity training provider or provided independently if the statewide training provider is incapable of providing the specific training.
E. Each agency shall identify roles with elevated privileges and responsibilities that introduce a higher level of risk and provide focused cybersecurity training before authorizing access to the system and at least annually thereafter. For example, executives, system administrators, etc.

IV. EXEMPTION PROCESS

Refer to ITA Policy P1010 (Data Technology Policies, Standards, and Guidelines Framework).

V. PROCEDURE REFERENCE

- National Institute of Standards and Technology (NIST) Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program – Provides guidance on developing security awareness and training programs.

VI. CONTACT DATA

For more data, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

08/20/2024 – Updated formatting to match current policy standards; removed information belonging in a standard; defined responsibilities of the State versus agencies.

07/01/2018 – Updated Idaho statute references.

Effective Date: February 23, 2016