Data Technology Authority (ITA)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4505 – Cybersecurity Awareness Training

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

II. ABSTRACT

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

The goal of awareness is to focus attention on security, 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

Each agency shall develop, document, and implement an agency-wide cybersecurity security awareness and training program. The security awareness program should be tailored to the information and information systems that support the operations and assets of the agency.

Agencies shall include cybersecurity awareness and training programs for all personnel using agency information assets consisting of;

- Cybersecurity risks associated with agency business operations,
- Compliance requirements with state and agency policies and procedures designed to reduce these risks,
- On-going security training for information systems support personnel, system administrators, and security managers appropriate to their roles and responsibilities.

Security awareness and training procedures shall be developed for the security program in general and (when required) for a particular information system.

Agencies shall ensure all system users are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.

Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.

Document, validate and improve cybersecurity awareness levels and training through periodic tests and evaluations. Targeted training should be provided to those who fail.

Identify personnel with significant information system support roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorizing access to the system and at least annually thereafter.

Determine the appropriate content of security awareness and training based on the specific requirements of the organization and the information systems to which personnel have authorized access.

Additional Guidance:
Security awareness topics may include (but are not limited to):

- Policies and Standards
- Incident response – reporting and handling
- Physical Security – facility access, visitor control, environmental risks, etc.
- Desktop security – allowed access to systems, use of screensavers, restricting view information on screen (preventing “shoulder surfing”), device locking
- Handheld device security – both physical and wireless security issues
- Individual accountability – identification and authentication; access to systems and data
- Access control issues – least privilege, separation of duties, etc.
- Information Protection – confidentiality concerns and controls.
- Encryption – transmission and storage of sensitive/confidential information.
- Information System Disposal – property transfer, media sanitization.

The following topics at a minimum should be addressed as baseline security training for all technical support personnel (system administrators, security administrators, network administrators, etc.):

- Protecting systems from malware.
- Data backup and storage.
- Timely application of system patches.
- Configuration/change management.
- Access control measures.
- Network infrastructure protection measures.

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) 332-1876.

REVISION HISTORY

Effective Date: February 23, 2016