Standard PR.AT: Cybersecurity Awareness and Training

February 10, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to
OCIO_IAS@ed.gov

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	12/9/19	Initial draft
1.1	2/12/2020	Underwent annual policy review for accuracy and timeliness.
1.2	2/2/2021	Underwent annual policy review for accuracy and timeliness and standardized in section 3, risk acceptance/policy exceptions.

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.10 19:06:21 -05'00'

_____ _____

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Table of Contents

1. INTRODUCTION

1.1 Purpose

This document establishes the Department standard for cybersecurity awareness and role-based training. In doing so, it supersedes any prior documentation establishing such standards.

1.2 Scope

This standard applies to all ED information system users, including employees, contract personnel, grantees, licensees, consultants, and any person or entity providing, operating, maintaining, or supporting systems that process ED information.

2. STANDARD

2.1 Cybersecurity and Privacy Awareness Training

a. The Department shall provide basic cybersecurity and privacy awareness training to all personnel and supporting contractors. The Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS) shall determine the appropriate content of security awareness training and security awareness techniques and the content shall:
    - Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents;
    - Address the need for awareness of operational security; and
    - Include content on recognizing and reporting potential insider-threat indicators.

b. All personnel and supporting contractors must complete OCIO/IAS published or authorized Cybersecurity and Privacy Awareness (CSPA) training prior to being granted access to any Department network or information systems and annually thereafter. No access will be granted until this requirement is fulfilled.

c. Annually all personnel and supporting contractors must complete OCIO/IAS published or authorized Cybersecurity and Privacy Awareness (CSPA) training to retain access to any Department network or information systems. Access will be revoked until this requirement is fulfilled.

d. Security awareness techniques such as information posted on ConnectED, generating email advisories/notices from senior Department officials, and conducting information security awareness events may be used to supplement training provided.

e. To reinforce cybersecurity and privacy awareness training provided, OCIO/IAS shall conduct practical exercises that simulate actual cyber-attacks. Practical exercises may

include social engineering attempts to collect information, gain unauthorized access, invoke opening malicious email attachments, or web links via spear phishing attacks.

2.2 Role-Based Security Training

a. Personnel and supporting contractors with Significant Security Responsibilities (SSR) are required to complete annual role-based security training.

b. The Office of Human Resources (OHR) shall identify all employees with SSR by mapping their job function to a work role and specialty area.

c. All companies/vendors contracting with ED are responsible for identifying their personnel who perform a role with SSR and must provide this information to their assigned Contracting Officer Representative (COR).

d. OCIO/IAS shall notify employees and contractors of their SSR designation and the associated training requirements. Further, OCIO/IAS shall identify role-based security training that will enable individuals with SSR to fulfill the information technology and cybersecurity responsibilities of their assigned functional roles.

2.3 Security Training Records

OCIO/IAS shall document and monitor individual information system security training activities, including basic security awareness training, practical awareness exercises, and role-based security training. Training records shall be maintained within the Department's authorized learning management systems or other authorized training record repository. Training records shall be maintained for a minimum of three years.

3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: RESOURCES AND REFERENCES

- NIST Special Publication (SP) 800-53, (as amended): *Security and Privacy Controls for Federal Information Systems and Organizations*