110 – Security Awareness and Training Standard

Purpose

The Security and Awareness Training Standard provides documentation of the minimum Information Technology (IT) Security Awareness Training for users of State information and information technology.

Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Literacy Training and Awareness (AT-2):

- Providing security and privacy literacy training to system users (including managers, senior executives, and contractors). Security and privacy training must be completed within 60 days of employment, when required by information system changes, and reinforced at least annually thereafter;
- Employing multiple techniques to increase the security and privacy awareness of system users. Techniques may include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices, and conducting awareness events;
- Updating literacy training and awareness content annually and following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
- Incorporating lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

Insider Threat (AT-2(2)):

- Providing literacy training on recognizing and reporting potential indicators of insider threat.

Social Engineering and Mining (AT-2(3)):

- Providing literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Role-Based Training (AT-3):

- Providing role-based security and privacy training to personnel (with Agency-defined roles and responsibilities) before authorizing access to the system, information, or performing assigned duties, annually thereafter, and when required by system changes;
- Updating role-based training content annually and following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
- Incorporating lessons learned from internal or external security or privacy incidents into role-based training.

Training Records (AT-4):

- Documenting and monitoring information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
- Retaining individual training records for five (5) years.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.

State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

Personally Identifiable Information, PII- For the purposes of this document PII includes the language in Wisconsin State Statute (CHAPTER 19 SUBCHAPTER IV) and applicable compliance regulations related to specific types of data, e.g. Criminal Justice Information, Federal Tax Information, and Protected Health Information.

Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies Exception Procedure.

Document History

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue

the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and Approved by:

Alan Greenberg, CISO — DocuSigned by: Alan Greenberg 706222F849B429... — 7/8/2022 | 1:55 PM CDT

Print/Type Title — Signature — Date