Effective: *08/08/2022*
Last Revised: *02/07/2023*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-05: Awareness and Training Standard

Standard Contents

1. Purpose

The purpose of the Awareness and Training Standard is to define the organization's requirements for the implementation and on-going management of an information security training and awareness program to educate users of information security risks and best practices. The standard outlines the methods and requirements for communicating with users about Executive Memoranda, Security Standards, and technology risks.

This standard is aimed to help reduce the risk of human error, theft, fraud, or misuse of University data. Security awareness training mandated by regulatory or industry requirements, including but not limited to, FERPA, HIPAA, PCI DSS, and ITAR, is in addition to the training for all system account holders and is the responsibility of the business entity subject to its compliance. This standard is intended to ensure that everyone is aware of roles and responsibilities and to the University's overall commitment to protecting its data.

2. Scope

This standard shall apply to all The University of Nebraska's ("The University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this Standard.

3. Standard Statement

It is the intention of this standard to establish a security awareness and training capability throughout The University to help document, communicate, and train university personnel on security best practices and concepts. All users with access to The University's Information Systems, and data shall undergo annual information security training and awareness. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (CISO) as defined in **ITS Policy Exception Standard**. The following subsections outline the Awareness and Training Standard.

4. Awareness and Training Requirements

4.1 Security and Awareness

4.1.1 Information Security Awareness and Training

The University's security awareness training will be managed by Information Technology Services (ITS). System account owners must complete a training and awareness course on information security risks and best practices, as well as organizational Executive Memoranda, standards, and procedures upon hiring and within thirty (30) days of employment, when required by information system changes, and then annually from then on.

4.1.2 Information Completion Tracking

Completion of the required training will be tracked by ITS Security Services. Completion of training activities must be documented and tracked to ensure that all users complete the necessary trainings in a timely manner. In the event that a user does not complete the required training(s), the user's supervisor shall be notified. In the event that the user does not complete the required training(s) within thirty (30) days of the annual due date, the user's access may be disabled until the required trainings are completed, however training can still be accessible.

A periodic report of new employees hired will be made available to the Security Awareness Manager, as designated by the CISO, to track completed trainings. Supervisors are responsible for ensuring that current employees under their supervision complete the University's security awareness training by the deadline set by the CISO.

4.1.3 Training Content

The ITS Chief Information Security Officer (CISO) or their designee is responsible for the development or acquisition of relevant training courses, maintaining training records, setting training deadlines, and providing such information to supervisors and system administrators.

All users shall be required to be trained on relevant information security risks and best practices, as well as relevant organizational policies and processes as dictated by Information Security, Compliance, and Human Resources. At a minimum, topics will include:

- Executive Memorandum 16
- Incident reporting procedures
- Password usage and management
- Unknown email attachments
- Social engineering, phishing, and spoofed emails
- Mobile device security
- Physical security and visitor control
- Social media use
- Data classifications and safe handling
- Secure work areas and traveling tips
- Legal requirements and regulations
- Implications of non-compliance with security policies
- Recognizing and reporting of potential insider threats

At the conclusion of the training, users must acknowledge that they have read and reviewed the Executive Memoranda, information security standards, and procedures.

All attendees shall be given the opportunity to provide Information Security / Human Resources with feedback regarding the training content and delivery method(s).

4.1.4 Role-Based Training

Job roles with greater inherent information security risks, responsibilities, and complexities shall require additional training beyond what is provided to all other users. This training is to be completed before authorizing access to the information system or performing assigned duties. These roles include, but are not limited to infrastructure administrators, individuals who have incident response responsibilities, developers, project/program managers, buyers etc. Information Security, Information Technology, and Compliance shall dictate whom requires role-based training, and how such trainings shall be sourced and facilitated.

Additional training may be required for individuals with access to personal health information (PHI) or credit card data:

- *Health Insurance Portability and Accountability Act (HIPAA) Training* – Required for employees involved with the use, processing, transmission, or storage of PHI.
- *Payment Card Industry (PCI) Training* – Required for employees who handle credit cards, manage credit card processes, or are responsible for or use POI (Point of Interaction) Credit Card devices.

4.1.5 Review of Training Content

The Information Security department must review the training plan, content, and feedback at least annually. Consideration must be given to any changes that may be warranted based on the received feedback, and/or any significant changes to the organization, information security threats, techniques, requirements, and responsibilities.

When reviewing the training plan, the aforementioned must consider how training is facilitated, who is required to attend training, how training is recorded and tracked, and the need to alter the training content.

4.1.6 Supplemental Awareness Initiatives

In addition to the use of a formal information security training course / curriculum, general security awareness must be communicated throughout The University’s environments utilizing periodic communications that may include, but are not limited to: scheduled awareness surveys, unscheduled awareness surveys, feedback surveys, e-mail advisories or newsletters, posters/ flyers, lunch-and-learn events, webinars, etc.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	02/07/2023
Approved by:	Bret Blackman	IT CIO	02/07/2023

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	2/7/2023	Revised language in section 4.1.2