THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0123-M - Security Awareness, Training, and Education Program	
Version: 8	Effective Date: 08/22/2024

Objective:

To establish a formal, documented Security Awareness, Training, and Education Program for information systems users and establish appropriate training controls for UTM.

Scope:

This program applies to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this policy is based on those guidelines. Specifically, this program is based on guidelines in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program.*

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a user accesses, uses, or handles University resources.

UT - Martin Policy: IT0123-M - Security Awareness, Training, and Education Program	
Version: 8	Effective Date: 08/22/2024

Program Details:

The Workforce and Sponsored Account Users shall successfully complete security awareness training annually. A reasonable amount of time will be granted to successfully complete the training in the specified Learning Management System (LMS). Information security awareness training will be used in personnel performance evaluations. Additional training will be required for individuals with certain roles and responsibilities within the University.

Roles and Responsibilities:

Chief Information Officer: Has overall accountability of this program as the Position of Authority.

Director of Infrastructure: Responsible for overseeing the implementation and maintenance of this program.

Deans, Directors, Department Heads/Chairs: Responsible for ensuring their employees complete the training before the deadline.

Account Sponsors: Responsible for ensuring the users whose accounts they sponsor complete the training before the deadline.

New Hires:

All new employees are required to complete security awareness training within 30 days of being hired (AT-2). The account expiration date will be set in Active Directory so if training hasn't been completed before the deadline, their account will be disabled. Their account will be reactivated temporarily until they successfully complete training. The expiration date will be removed once the user has passed their required security awareness training.

Required Training:

The Workforce is required to successfully complete the "General Employee Security Awareness Training" each calendar year (AT-2). These users have the option of passing the PreCheck but must complete any advanced training assigned to them.

Post-Retirement Users are considered Workforce and must comply with those requirements.

Sponsored Account Users will be required to complete alternative training modules assigned specifically to them.

Advanced Training:

In addition to the "General Employee Security Awareness Training," all ITS staff shall complete the "IT Employees Security Awareness Training." All executives/administration and managers shall complete the "Exec/Admin Security Awareness Training" (AT-3).

PreCheck is only available for the "General Employee Security Awareness Training" and does not exempt users from advanced training requirements.

ITS student workers shall complete additional training that could be provided outside the specified LMS.

Third-Party Users:

Third-party users shall complete training prior to accessing the network or systems. Users from other UT campuses and institutes must complete security awareness training from their respective campus or institute and provide a certificate of completion.

Visitors:

Visitors to campus are not required to complete security awareness training but are only permitted to use the publicly accessible computers in the library, the guest wireless network, or the Eduroam wireless network.

Tracking Participation:

The LMS used to provide training content shall have the ability to monitor and report compliance and progress (AT-4). Participation in security awareness training can be documented for credit in accordance with UT policy HR0128 unless it was required by sanctions.

Evaluation and Feedback:

Mechanisms for evaluation and feedback should be implemented into training to help determine effectiveness and quality.

Updating:

Training content and delivery should be evaluated at least yearly. Additional evaluation may be necessary with changes in:

- Updated content
- Platform
- Policies, standards, guidelines
- Legal requirements
- Assessment or audit findings
- Security incidents or breaches

Sanctions for Non-Completion of Annual Training:

Sanctions will be imposed against users who do not complete the required annual training before the deadline (PS-8).

Workforce (including Post-Retirement Users):

1st Missed Deadline:

- Account is disabled at midnight
- Immediate supervisor must contact the Help Desk to request account reactivation
- All required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:

- Account is disabled
- Dean or Department Head must contact the Help Desk to request account reactivation
- All required training must be completed within 24 hours

3rd Missed Deadline:

- Account is disabled
- Non-compliance reported to the appropriate vice-chancellor by the respective Dean or Department Head
- Employee is required to meet with their Dean or Department Head and Security Administrator before account reactivation – facilitated by the Dean or Department Head
- Employee receives a written warning from their Dean or Department Head that is to be included in their departmental personnel file
- All required training must be completed by the end of the workday (5:00PM CDT/CST)

4th Missed Deadline:

- Account is disabled
- Network access for all the employee's registered devices is disabled
- To be determined by the appropriate vice-chancellor

Sponsored Account Users (includes Retirees):

1st Missed Deadline:

- Account is disabled at midnight
- Account sponsor must contact the Help Desk to request account reactivation
- Required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:

- Account is disabled
- Account Sponsor must contact the Help Desk to request account reactivation
- Required training must be completed within 24 hours of account reactivation

3rd Missed Deadline:

- Account is disabled
- LMS is checked for logins and attempts
- User is contacted to see if there were any extenuating circumstances, etc. preventing them from completing training. The user must choose a day within 7 days to complete all required training by 5:00 PM CT on that day.

4th Missed Deadline:

- Account is disabled
- To be determined by the CIO

Third-Party Users:

1st Missed Deadline:

- Account is disabled

New Hires:

Sanctions will be imposed against new hires who do not complete the required training within 30 days of being hired (AT-2).

1st Missed Deadline:
- Account is disabled
- Immediate supervisor must contact the Help Desk to request account reactivation
- All required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:
- Account is disabled
- Dean or Department Head must contact the Help Desk to request account reactivation
- All required training must be completed within 24 hours

3rd Missed Deadline:
- Account is disabled
- Non-compliance reported to the appropriate vice-chancellor by the respective Dean or Department Head
- Employee is required to meet with their Dean or Department Head and Security Administrator before account reactivation – facilitated by the Dean or Department Head
- Employee receives a written warning from their Dean or Department Head that is to be included in their departmental personnel file
- All required training must be completed by the end of the workday (5:00PM CDT/CST)

4th Missed Deadline:
- Account is disabled
- Network access for all the employee's registered devices is disabled
- To be determined by the appropriate vice-chancellor

Sanctions for Compromised Accounts:

Sanctions will be imposed against users who allow their accounts to be compromised and are dependent on the number of occurrences (PS-8). The severity of an incident can also be used for determining sanctions. Re-testing for sanctions does not apply toward the annual requirement.

Workforce (including Post-Retirement Users):

1st Offense:
- Complete all assigned security awareness training within 24 hours

2nd Offense:
- Actions are reported to the employee's Dean or Department Head by their immediate supervisor
- Additional security awareness training may be required

3rd Offense:
- Actions are reported to the appropriate vice-chancellor by the respective Dean or Department Head
- Employee receives a written warning from the Dean or Department Head that is to be included in the departmental personnel file
- Internet access is restricted until one-on-one training with a member of ITS security staff is completed

4th Offense and beyond:
- To be determined by the appropriate vice-chancellor

Sponsored Account Users:

1st Offense:
- Complete all assigned security awareness training within 24 hours

2nd Offense:
- Account access is restricted until alternative training is completed

3rd Offense:
- Account is disabled
- To be determined by the CIO

Third-Party Users:

1st Offense:
- Network access is revoked

Practical Exercises (AT-2):

ITS Security can perform various exercises to test the effectiveness of the security awareness training. Prior notice to and approval from the CIO and Director of Infrastructure is required before proceeding with any practical exercises.

Users who fail practical exercises and/or have their accounts compromised may be subject to additional exercises and/or training.

References:

IT0123 - Security Awareness, Training, and Education

HR0128 - Employee Professional Development and Training

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program

NIST SP 800-16 Revision 1 (3rd Draft), A Role-Based Model for Federal Information Technology / Cybersecurity Training

NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations

Definitions:

Eduroam: A global wireless network access service for research and education organizations to provide students, researchers, staff, and faculty with wireless access at participating institutions using their home campus / institution credentials.

Employee: Faculty, staff, student worker, post-retirement user.

Learning Management System (LMS): A software application or online platform that facilitates the administration, delivery, and management of educational courses, training programs, or learning materials.

Multi-Factor Authentication (MFA): A method of confirming a user's claimed identity by requiring a combination of two or more different authentication factors, which includes something you know (password, PIN), something you have (smart card, token), and something you are (biometrics).

Post-Retirement User: An employee who retires from the University of Tennessee and returns to employment in a temporary status.

Sanction: An official action taken against a user.

Sponsored Account User: Retiree, family member, or non-employee account holder.

Third-Party User: An authorized user not affiliated with the university but involved in collaboration, including but not limited to auditors, consultants, vendors, and contractors.

Visitor: A user not directly affiliated with the University.

Workforce: All current faculty, staff, ITS student workers, and post-retirement users.