Objective:

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

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 remote 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.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

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.
Program Details:

The campus Workforce and Affiliates must successfully complete security awareness training annually. A reasonable amount of time will be granted to successfully complete the training in the current Learning Management System (LMS). Information security awareness training will be used in personnel performance evaluations. Additional training will be required for individuals with specific roles and responsibilities within the University.

Workforce:

The Workforce at UTM consists of all current faculty, staff, and ITS student workers.

Affiliates:

Affiliate users consist of retirees, family members, and friends of the university with UTM email accounts.

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 the security awareness course in the LMS.

Required Training:

The Workforce and Affiliates are required to successfully complete the “Required Core” module each calendar year (AT-2).

Advanced Training:

All ITS staff and student workers, executives, and managers must also successfully complete the “Required Advanced” module in addition to “Required Core” (AT-3).

Third-Party Users:

Third-party users must complete training prior to accessing the network or systems (AT-3). Third-party users from other UT campuses or institutes are exempt from completing training provided they have completed security awareness training from their respective campus or institute.
Visitors:

Visitors to campus are not required to complete security awareness training. They are only permitted to use the publicly accessible computers in the Library, the “UTM Guest” wireless network, or Eduroam if they are from a participating institution.

Tracking Participation:

The LMS used to provide training content must 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 will be necessary with changes in:

- Updated content
- Platform
- Policies
- Legal requirements
Sanctions for Non-Completion of Annual Training:

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

Workforce:

1st Missed Deadline:
  - Account is disabled at midnight
  - All required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:
  - Account is disabled
  - Non-compliance reported to the department head, Department Chair and/or Dean of the College
  - Immediate supervisor or department head must request account reactivation and all required training must be completed within 24 hours

3rd Missed Deadline:
  - Account is disabled
  - Non-compliance reported to the appropriate vice-chancellor
  - Employee is required to meet with their supervisor, department head, Department Chair and/or Dean of the College, and Security Administrator before account reactivation
  - Employee receives a written warning that is to be included in the departmental personnel file
  - All required training must be completed by the end of the workday

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

Affiliates:

1st Missed Deadline:
  - Account is disabled at midnight
  - Required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:
  - Account is disabled
  - Required training must be completed within 24 hours of account reactivation

3rd Missed Deadline:
  - Account is permanently disabled
Third-Party Users:

1st Missed Deadline:
- Account is disabled

New Hires:

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

1st Missed Deadline:
- Account is disabled
- Incident reported to immediate supervisor or department head
- All required training must be completed within 48 hours of account reactivation

2nd Missed Deadline:
- Account is disabled
- Non-compliance reported to the department head, Department Chair and/or Dean of the College
- Immediate supervisor or department head must request account reactivation and all required training must be completed within 24 hours

3rd Missed Deadline:
- Account is disabled
- Non-compliance reported to the appropriate vice-chancellor
- Employee is required to meet with their supervisor, department head, Department Chair and/or Dean of the College, and Security Administrator before account reactivation
- Employee receives a written warning that is to be included in the departmental personnel file
- All required training must be completed by the end of the workday

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 implemented 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:

1st Offense:
- Actions are reported to immediate supervisor or department head
- Complete Required Core module for security awareness within 48 hours
- User enrolled in 2FA

2nd Offense:
- Actions are reported to the department head, Department Chair, and/or Dean of the College
- Complete “Required Core” module for security awareness within 24 hours
- Additional training may also be recommended or required

3rd Offense:
- Actions are reported to the appropriate vice-chancellor
- Employee receives a written warning 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

Affiliates:

1st Offense:
- Complete “Required Core” module for security awareness
- User enrolled in 2FA (dependent on the current licensing structure)

2nd Offense:
- Network access is restricted until specialized training is completed

3rd Offense:
- Permanent revocation of network access privileges

Third-Party Users:

1st Offense:
- Network access is revoked
Practical Exercises (AT-2.1):

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

Mandatory Controls:

Mandatory security controls are University-wide controls that are required to be consistently designed, implemented, monitored, and assessed.

Workforce Designation: Each Campus must designate the makeup of its Workforce requiring Awareness Training.

Basic Security Awareness Training (AT-2): Basic security awareness training as a part of initial training for new users, when it is required by information system changes, and annually thereafter.

Role-based Security Training (AT-3): Each Campus must provide role-based security training to personnel with assigned security responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes, and annually thereafter.

Security Training Records (AT-4): Each campus must document and monitor individual information system user security training activities.

Discretionary Controls:

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

Security Awareness Training | Practical Exercises (AT-2.1): Practical exercises include but are not limited to, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Personnel Sanctions (PS-8): Formal sanctions processes for personnel failing to comply with established information security policies and procedures.
UT - Martin Policy:
IT0123-M - Security Awareness, Training, and Education Program

Version: 5  Effective Date: 06/08/2020

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 4 - Recommended Security Controls for Federal Information Systems and Organizations

Definitions:

Affiliate: Retiree, family member, or friend of the university who has a UTM email account.

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 through the use of their home institution credentials.

Employee: Faculty, staff, or student worker

Sanction: An official action taken against a user

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.

Two-Factor Authentication (2FA): A method of confirming a user's claimed identity by requiring a combination of two different components, which includes something you know (password, PIN), something you have (smart card, token), and something you are (biometrics).

Visitor: A user not directly affiliated with the university.

Workforce: All current faculty, staff, and ITS student workers.