SECURITY AWARENESS, TRAINING, AND EDUCATION PLAN

Version 1.7
JUNE 2016
# TABLE OF CONTENTS

1.1 Scope 3

1.2 Principles 3

1.3 Revisions 4

2.1 Objective 5

3.1 Plan Details 5

3.2 New Hires 5

3.3 Employees and Retirees 5
   3.3.1 IT Staff 5

3.4 Third-Party Users 5

3.5 Visitors 6

3.6 Participation Tracking 6

3.7 Evaluation and Feedback 6

3.8 Updating 6

3.9 Sanctions 6
   3.9.1 Faculty and Staff 6
   3.9.2 Retirees 7
   3.9.3 Third-Party Users 7

3.10 Practical Exercises 7

4.1 Mandatory Controls 7

5.1 Discretionary Controls 8

6.1 References 8

7.1 Definitions 9
1.1 SCOPE
This plan 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.

1.2 PRINCIPLES
UTM 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 policy is based on guidelines in NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/10/2016</td>
<td>Created (1.0)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>08/03/2016</td>
<td>Content, wording (1.1)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>08/03/2016</td>
<td>Submitted for preliminary review</td>
<td></td>
</tr>
<tr>
<td>08/26/2016</td>
<td>Wording, formatting (1.2)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>08/31/2016</td>
<td>Third-party users, security controls (1.3)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Mandatory and discretionary controls, recommended changes, visitors (1.4)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>11/17/2016</td>
<td>Eduroam definition, executive and management subsection (1.5)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>11/18/2016</td>
<td>Changed to plan (1.6)</td>
<td>Brian Stubblefield</td>
</tr>
<tr>
<td>11/21/2016</td>
<td>Practical exercises, LMS, HR0128 reference, sanctions, title (1.7)</td>
<td>Brian Stubblefield</td>
</tr>
</tbody>
</table>
2.1 OBJECTIVE
To establish a formal, documented Security Awareness, Training, and Education program for University information systems users, and facilitate appropriate training controls.

3.1 PLAN DETAILS
All employees and retirees must successfully complete security awareness training once each calendar year. University employees and retirees will be granted a reasonable amount of time 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.

3.2 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.

3.3 EMPLOYEES AND RETIREES
All employees and retirees are required to successfully complete the “Required Training” module each calendar year (AT-2). Re-testing for sanctions does not apply toward the annual requirement.

3.3.1 IT STAFF
All ITS staff and student workers must successfully complete the “IT Staff” module in addition to the required yearly training (AT-3).

3.3.2 EXECUTIVE & MANAGEMENT
All executives and managers must successfully complete the “Executive and Management” module in addition to the required yearly training (AT-3).

3.4 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.
### 3.5 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.

### 3.6 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.

### 3.7 EVALUATION AND FEEDBACK
Mechanisms for evaluation and feedback should be implemented into training to help determine effectiveness and quality.

### 3.8 UPDATING
Training content and delivery should be evaluated at least yearly. Additional evaluation will be necessary with changes in:
1. Updated content
2. Platform
3. Policies
4. Legal requirements

### 3.9 SANCTIONS (PS-8)
Sanctions will be implemented against users who allow their accounts to be compromised and are dependent on the number of occurrences. The severity of an incident can also be used for determining sanctions.

#### 3.9.1 FACULTY AND STAFF
1st Offense:
- Actions are reported to immediate supervisor or department head
- Retake security awareness training
2nd Offense:
- Actions are reported to the department head, Chair of the Department, and/or Dean of the College
- Retake security awareness training
- Additional training may also be recommended or required
3<sup>rd</sup> Offense:
- Actions are reported to the appropriate vice-chancellor
- Notation is made in the offender’s Human Resources file
- Internet access is restricted until one-on-one training with a member of ITS security staff is completed

4<sup>th</sup> Offense and beyond:
- Determined by the appropriate vice-chancellor

3.9.2 RETIREES
1<sup>st</sup> Offense:
- Retake security awareness training

2<sup>nd</sup> Offense:
- Network access is restricted until one-on-one training with a member of ITS security staff is completed

3<sup>rd</sup> Offense:
- Permanent revocation of network access privileges

3.9.3 THIRD-PARTY USERS
1<sup>st</sup> Offense:
- Network access is revoked

3.10 PRACTICAL EXERCISES (AT-2(1))
ITS Security can perform certain exercises to test the effectiveness of the security awareness training on a group of or individual users. Prior notice to and approval from the CIO and Director of System Administration and Security is required before proceeding with any practical exercise.

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

- **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.
5.1 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.

- **Personnel Sanctions (PS-8):** Formal sanctions processes for personnel failing to comply with established information security policies and procedures.

- **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.

6.1 REFERENCES

IT0123 – Security Awareness, Training, and Education

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

NIST SP 800-16 Rev1, 3rd Draft - A Role-Based Model for Federal Information Technology/Cybersecurity Training

NIST SP 800-53 Rev4 - Recommended Security Controls for Federal Information Systems and Organizations

HR0128 - Human Resources Development
7.1 DEFINITIONS

**Eduroam**: (education roaming) is a secure roaming access service which allows students and staff from participating institutions to obtain Internet connectivity when visiting participating institutions using their own 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.

**Visitor**: A user not directly affiliated with the university.