THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0123 - Security Awareness, Training, and Education	
Version: 4	**Effective Date: 01/12/2018**

IT0123 - Security Awareness, Training, and Education

Objective:

To establish policy for maintaining the security skills of the University's Workforce.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

“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 (NIST) 800 series of publications, and this policy is based on those guidelines.

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.

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy.

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 IT resources.

Policy:

Each of the University's Campuses must develop or adopt and adhere to a formal, documented Security Awareness and Training program for their Workforce, and facilitate appropriate training controls.

Mandatory Controls:

Mandatory security controls are University-wide controls that are required to be consistently designed, implemented, monitored, and assessed by all Campuses. Each Campus must develop, document, and maintain a Security Awareness and Training program that includes:

1. **Workforce Designation:** Each Campus must designate the makeup of its Workforce requiring Awareness Training.
2. **Basic Security Awareness Training** (AT-2): Each Campus must assure basic security awareness training is provided as a part of initial training for new members of the Workforce, when it is required by information system changes, and annually thereafter.
3. **Role-based Security Training** (AT-3): Each Campus must provide role-based security training to Workforce members with assigned security responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes, and annually thereafter.
4. **Security Training Records** (AT-4): Each campus must document and monitor its Workforce information 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.

References:

1. NIST 800-53 *"Recommended Security Controls for Federal Information Systems and Organizations"*
2. NIST 800-50 *"Building an Information Technology Security Awareness and Training Program"*
3. NIST 800-16 *"A Role-Based Model for Federal Information Technology / Cyber Security Training"*

Revisions:

10/1/2014	Effective
1/5/2016	Updated 1.c to clarify "periodically" to be "at least annually."
9/19/2016	Added Mandatory Controls and Discretionary Controls Sections.
7/20/2017	Adjusted policy to allow Campuses to designate the Workforce needing training.
1/10/2018	Reviewed and approved