THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0014 - Information Technology Security Awareness Training Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure to the University to establish an information technology security awareness program strategy that enhances the ability to recognize threats and react accordingly.

II. Security Awareness Training Policy

The Central IT Department must communicate the requirements and processes for security awareness training management to the campus community annually to engage campus communities and individuals in the shared responsibility of security awareness training management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. The Central IT Department will create a process for performing security awareness training that is documented and approved by the campus or institute CIO/DTL. Training should be based on the highest risks to the University and the training may change based on risk assessments (reference the System-wide Policy: IT0004 – Information Technology Risk Management for more information on risk management).

2. University Employees (Employees) must complete security awareness training, at a minimum, on an annual basis.

a. All new Employees must complete cybersecurity awareness training within 30 days of being granted access to the University's Assets.

b. Employees must be trained in how to recognize social engineering attacks.

c. Employees must be trained in the best practices for authentication to the University's Resources.

d. Employees must be trained in the best practices for handling the University's Data that provides clear guidance based on the categorization of the Data (reference System-wide Policy: IT0005 – Data Categorization for more information on data categorization).

3. Training must be included on the following subjects as it pertains to the University's Data Management Policy (reference System-wide Policy: IT0311 - Information Technology Data Access, Management, and Recovery):

i. Identifying Protected University Data.

ii. Storing Protected University Data.

iii. Transferring Protected University Data.

iv. Archiving Protected University Data.

v. Destroying Protected University Data.

vi. Any legal and/or regulatory obligations of the above.

4. Clear screen and clean desk best practices must be included in the training and include the timeframes for automatic session locking the University's Assets (reference the System-wide Policy: IT4912 - Information Technology Secure Configuration Management).

5. Employees must be trained on the causes of unintentional Data exposure in the University.

6. Employees must be trained in how to recognize and report security incidents.

7. Employees must be trained in how to identify and report if the University's Assets are missing security updates (reference the System-wide Policy: IT4912 - Information Technology Secure Configuration Management).

8. Employees must be trained in the dangers of connecting to and transmitting University Data over insecure IT Networks.

9. Failure of an Employee to complete the mandatory training requirements defined by the Central IT Department will result in User Account disablement.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

10. The Central IT Department will create a process to conduct role-specific security awareness and skills training (IG2).

III. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for information technology security awareness training management as described in CIS Control 14 (Security Awareness and Skills Training) for the University of Tennessee in support of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy applies to all University Employees.

SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[Text Wrapping Break]_____

SECTION 8. Policy History

Revision 1:

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0005 – Data Categorization

f. IT0017 – Information Technology Incident Response Management

g. IT0102 – Information Technology Asset Management

h. IT0311 – Information Technology Data Access, Management, and Recovery

i. IT0506 – Information Technology Account and Credential Management

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration

k. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/
