EAST TENNESSEE STATE
UNIVERSITY

Cybersecurity Awareness Training Program

Policy Effective Date: 5/13/2019 • **Policy Revised:** 5/10/2022
Procedures Effective Date: 5/13/2019 • **Procedures Revised:** 5/10/2022

Policy Name: Cybersecurity Awareness Training Program

Policy Purpose

This policy outlines the ETSU Cybersecurity Awareness and Training Program (CSAT Program). The CSAT Program is implemented by the Office of Information Technology Services (ITS) to inform and educate all employees of their information security obligations, and to reduce the security risks to ETSU systems and data.

Applicability

This policy is applicable to employees.

Responsible Official, Office, and Interpretation

The Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer, in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Single Sign-On (SSO)

Login method that allows users to log in to multiple applications using one set of credentials.

Policy Name: Cybersecurity Awareness Training Program

Policy

ITS defines and ensures the implementation of a cybersecurity awareness training program to increase individual awareness of information security responsibilities regarding protection of the confidentiality, integrity, availability, and appropriate use of ETSU information resources. All ETSU employees must complete the CSAT Program regardless of whether they use ETSU computer and networks.

ITS will document and monitor individual information system security training activities, including basic security awareness training and specific information system security training. ETSU will retain training records for three years.

1. Required Training.

Mandatory CSAT Program training is provided in an appropriate form based on ETSU's needs regarding emerging security threats and data obtained from the Cybersecurity Awareness Training System (System) and various cybersecurity intelligence and law enforcement agencies. Such training may include short informational videos or illustrations, phishing campaigns, and social engineering experiments.

Employee accounts are automatically onboarded into the System. The System sends a welcome email, followed by reminder emails at 6-day intervals or less, until compliance is achieved. CSAT Program training shall be completed within sixty (60) days of the date of hire. Thereafter, CSAT Program refresher training shall be completed annually, and within sixty (60) days of the anniversary of the previous campus-wide training campaign. Additional training may be required for information system changes and as needed thereafter, or as otherwise determined necessary by the Chief Information Officer (CIO).

2. Additional Training Required.

Additional role-based security awareness training is required for employees whose responsibilities require elevated access or privileged access, including access to regulated or confidential information, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and related information systems. Further role-based security awareness training may be mandated at the discretion of the CIO. This training must be completed annually or periodically, as required by the relevant regulatory or contractual compliance programs, or as determined by the CIO.

3. Ongoing Training.

Training occurs at least once annually for all ETSU employees based on this policy, and state and cybersecurity insurance requirements. Alternate delivery methods for completion of the required training, such as ITS group training sessions, may be approved. The frequency and method of delivery of ongoing training may be altered based on emerging security threats and data obtained from the System and other intelligence sources.

4. Tracking, Evaluation, and Feedback.

The System tracks users' training progress and users' susceptibility to social engineering attacks to validate training effectiveness and help improve training delivery. The System provides reports on individual training compliance and assigns risk ratings to individual users based on individual responses to training. Individuals may be assigned additional relevant security training if deemed necessary.

5. Non-Compliance.

ITS shall limit network access of individuals not in compliance with this policy or take other necessary action to protect the security of information systems and data. ETSU Single Sign-On (SSO) access is limited to CSAT Program training material when individual compliance falls past due. Regular SSO access is automatically restored following compliance. A grace period of up to thirty (30) days for the completion or re-completion of CSAT Program training may be requested by the individual's supervisor, submitted to ITS through the individual's respective Vice President or their designee.

Procedures

N/A

Applicable Forms and Websites

ETSU Cybersecurity Awareness website

Authority and Revisions

Authority: Authority T.C.A. § 49-8-203 et seq., T.C.A. § 47-18-2107, Health Insurance Portability and Accountability Act (HIPAA) found at 45 CFR 160, 162, and 164.

Previous Policy: N/A

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational programs and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.