Information Security Awareness Training Program (ISAT Program)	
Responsible Official: Chief Information Officer	**Responsible Office**: Information Technology Services

Policy Purpose

This policy establishes the East Tennessee State University (ETSU) Information Security Awareness and Training Program (ISAT Program). The ISAT Program is implemented by the Office of Information Technology Services (ITS) and is intended to inform and educate all employees and third parties on their information security obligations, and to reduce the security risks to ETSU systems and data.

This policy specifies procedures for informing ETSU employees and third parties of system security requirements and their individual responsibilities to protect information technology systems and data commensurate with their roles at ETSU. It also describes the security awareness and training controls that will be established to protect the confidentiality, integrity, and appropriate use of ETSU information resources.

Policy Statement

I. Applicability

This policy applies to all ETSU employees, regardless of whether they use ETSU computer systems and networks. All employees are expected to protect all forms of information assets, including computer data, written materials, paperwork, and intangible knowledge and experience. This policy also applies to third parties working for or on behalf of ETSU with access to ETSU resources, whether they are explicitly bound (e.g., by contractual terms and conditions) or implicitly bound (e.g., by generally held standards of ethics and acceptable behavior) to comply with ETSU information security policies.

II. Policy

The Chief Information Security Officer (CISO), on behalf of ETSU, shall define and ensure the implementation of an ISAT Program to increase individual awareness of information security responsibilities with regard to protecting the confidentiality, integrity, availability, and

appropriate use of ETSU information resources. All ETSU employees, including temporary and student employees, and certain third parties, shall complete the ISAT Program:

- Before being authorized access to an information system or performing assigned duties;
- When required by information system changes;
- As needed thereafter; and
- As otherwise determined necessary by the CISO.

ISAT Program training shall be completed within thirty (30) days from the date of hire. Thereafter, ISAT Program refresher training shall be completed annually, and within sixty (60) days of the anniversary of the previous instance of such training.

Additional role-based security awareness training shall be required for employees or third parties whose responsibilities require elevated access, including access to regulated or confidential information, such as HIPAA, PCI-DSS, and related Information Systems. Additional role-based security awareness training may be required at the discretion of the CISO. Role-based training shall be completed on an annual or periodic basis, as required by the relevant regulatory or contractual compliance programs, or as determined by the CISO.

ETSU will review and update this policy and procedures as needed. Additionally, 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.

III. Non-compliance

The CISO is authorized to 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. The individual's supervisor may request a grace period for completion or re-completion of ISAT Program training, not not to exceed thirty (30) days, through the respective Vice President. In cases where ETSU resources are actively threatened, the CISO will act in the best interest of the University by securing the resources in a manner consistent with the Cybersecurity Incident Response Plan.

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.

Defined Terms

Phishing emails	Emails purporting to be from reputable companies in order to induce individuals to reveal confidential or personal information, such as passwords and credit card numbers.

Social engineering	The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Policy History

Effective Date: May 13, 2019

Revised Effective Date:

Procedure (s)

ISAT Program Required training

1. Review and acceptance of the University policy on Acceptable Use of Technology
2. Security Awareness training videos.
    a. New employees and certain third-party accounts are automatically onboarded into the Information Security Awareness Training System (System).
    b. The System sends email notifications to new accounts 30, 20, 10, 7, 5, 3, 2, and 1 day before the signature deadline or until the required action is completed.
    c. Network access is limited to computer and wireless logins until the individual is compliant.
    d. Access to sensitive systems such as the University Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Financial Systems is enabled after the University Acceptable Use of Technology policy has been electronically signed.

The CISO provides mandatory ISAT Program training in an appropriate form based on ETSU's needs regarding emerging security threats and data obtained from the System. Such training may include (e.g.) short informational videos or illustrations, phishing campaigns, and social engineering experiments.

Ongoing training

The frequency and method of delivery of ongoing training shall be determined by the CISO based on ETSU's needs regarding emerging security threats and data obtained from the System.

Tracking, Evaluation, and Feedback

The ISAT Program System will track users' training progress and users' susceptibility to social engineering attacks to validate training effectiveness and help the CISO improve training delivery. The System provides reports to the CISO on individual training compliance and assigns risk ratings to individual users based on individual responses to training. The System automatically enrolls at-risk individuals for additional relevant security training as needed to

ensure individuals are effectively training and to protect the confidentiality, integrity, and availability and assure the appropriate use of ETSU Information Resources.

Procedure History

Effective Date: May 13, 2019

Revised Effective Date:

Related Form(s)

Scope and Applicability

Check those that apply to this policy and identify proposed sub-category.

	Governance	
	Academic	
	Students	
	Employment	
X	Information Technology	
	Health and Safety	
	Business and Finance	
	Facilities and Operations	
	Advancement	