EAST TENNESSEE STATE
UNIVERSITY

Information Security Awareness Training	
Responsible Official: Chief Information Officer	Responsible Office: Information Technology Services

Policy Purpose

This policy establishes the University’s Information Security Awareness And Training Program (“Program”). The Program is intended to inform and educate all employees and third parties on their information security obligations and reduce risk to University systems and data. This policy specifies procedures for informing university employees and third parties of system security requirements and their individual responsibilities to protect information technology (“IT”) 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, availability, and appropriate use of University Information Resources.

Policy Statement

I. Applicability

This policy applies to all University employees, regardless of whether they use 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 the University with access to University 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 University information security policies.

II. Policy

The Chief Information Security Officer (CISO), on behalf of the University, shall define and ensure the implementation of an Information Security Awareness Training Program (“Program”) to increase individual awareness of information security responsibilities in regard to protecting the confidentiality, integrity, availability, and appropriate use of University Information Resources. As part of the Program, all University employees, including temporary and student employees and certain third parties, shall complete security awareness training

- 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.

Security Awareness training shall be completed within 30 days from the date of hire. Thereafter, Security Awareness Refresher Training shall be completed annually, within 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.

The University will review and update this policy and procedures as needed. Additionally, Information Technology Services will document and monitor individual information system security training activities, including basic security awareness training and specific information system security training, and 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. An individual's supervisor may request a grace period for completion or re-completion of security awareness training not exceeding 30 days through the respective Vice President. In cases where University 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.

Definitions

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:
Revision Date:

Procedure (s)

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 will automatically be onboarded into the Information Security Awareness Training System ("System").

b. The System will send 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 will be 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 will only be enabled after the University Acceptable Use of Technology policy has been electronically signed.

The CISO will provide mandatory security awareness training in an appropriate form based on the University’s needs, taking into account 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 the University’s needs, taking into account emerging security threats and data obtained from the System.

Tracking, Evaluation, and Feedback

The security awareness training 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 will provide reports to the CISO on individual training compliance and will assign risk ratings to individual users based on individual responses to training. The System will automatically enroll at-risk individuals for additional relevant security training as needed to ensure individuals are effectively trained and to protect the confidentiality, integrity, and availability and assure the appropriate use of University Information Resources.

Procedure History

Effective Date:
Revision Date:

Related Form(s)