



EAST TENNESSEE STATE
UNIVERSITY

Information Security

Policy Name: Information Security

Policy Purpose

This policy specifies the framework for implementing a university-wide, comprehensive, standards-based information security program to protect the information that is critical to teaching, research, and the university's varied activities, its business operation, and the communities it supports, including students, employees, and the public. These protections may be governed by legal, contractual, or East Tennessee State University policy considerations.

Applicability

This policy is applicable to students, employees, visitors, and third-party personnel.

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.

N/A

Policy Name: Information Security

Policy

It is ETSU's policy to support a comprehensive, University-wide, information security program consisting of measures that protect the confidentiality, integrity, and availability of the organization's data and information systems essential to the mission and institutional strategic goals of ETSU. System and data owners should refer to the [ETSU Business and Finance Records Classification Guide](#) regarding classification, retention, and disposal of university data.

ETSU implements information security and privacy programs aligned with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. Risk management, information security, and privacy programs shall align with the University's mission and its strategic goals, while taking into consideration the University's risk tolerance and finding the appropriate balance between security, University requirements, applicable regulations, and academic freedom.

Information security is a shared responsibility of the entire ETSU community. All university members have a responsibility for the proper handling and protection of ETSU data and systems. All university members are obligated to report cybersecurity breaches or expected breaches.

Policy Name: Information Security

Procedures

N/A

Applicable Forms and Websites

[ETSU Business and Finance Records Classification Guide](#)

Authority and Revisions

Authority: Focus Act § 49-8-203 et. seq; National Institute of Standards and Technology (NIST) 800 series.

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.