THE UNIVERSITY OF TENNESSEE

System-wide Policy:
IT0004 - Information Technology Risk Management

Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to establish a risk-based Information Technology Security Program Strategy for the University.

II. Risk Management Policy

Each of the University's campuses and institutes must maintain a formal, documented IT Risk Management program that ensures the implementation of appropriate and effective controls for the University's Resources based on risk.

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

Risk Management is a lifecycle approach and not a single point of time evaluation. It is the responsibility of the campus or institute CIO/DTL to ensure IT risk is managed and mitigated.

1. All Risk Management programs will follow the CIS Risk Assessment Method (RAM) unless there is a contractual and/or governmental requirement to use another methodology and address physical, as well as Data and System risks associated with IT Resources. Where appropriate, additional risk management methodologies can augment CIS RAM.

2. All Risk Assessments will be catalogued in a central repository.

3. The Data Owner(s) or Data Steward(s) must be consulted as a part of the Risk Assessment and must provide input to the impact portion of the assessment.

4. The Data Flows must be mapped as a part of the Risk Assessment process to determine the risks associated with the transmission, processing, and storage of the Data.

5. The Data Custodian(s) must be consulted as a part of the Risk Assessment and must provide input to the Safeguard Maturity determination.

6. All campus and institute Risk Management programs must include:

a. Risk assessments must be conducted on a regular interval and when changes to the system occur.

i. Systems that store, process, or transmit Data categorized as Private (Level 2) or Restricted (Level 3) for confidentiality and integrity should occur more frequently than for systems that store, process, or transmit Data categorized as Public (Level 0) or Internal Use Only (Level 1).

ii. Risk Assessment intervals must comply with regulatory or contractual requirements.

iii. Risk Assessments must be conducted on systems that store, process, or transmit Data categorized as Public (Level 0) or Internal Use Only (Level 1) only when changes to the system occur.

b. A process for Risk Assessment as a part of the procurement review process.

c. A process for Risk Assessment as a part of the configuration and change management processes.

7. The Risk Management program will include the following:

a. A process to document, track, and ensure that the Risk Assessments are updated per sections 3.a.i through 3.a.iii above or when significant changes are made to Systems or their operational environment, that pose new Threats and Vulnerabilities.

b. A process to document and disseminate Risk Assessment results to appropriate management and System and Data Custodians.

c. A process to track risk mitigation for each risk found, including providing documentation on acceptance of risk by the campus or institute leadership.

d. The Central IT Department will create a process to report all risk management efforts to the Enterprise Risk Officer for the University of Tennessee System on an annual basis.

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 Risk Management 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 Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

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 #:

____

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 and Computer System Categorization

f. IT0014 – Security Awareness Training Management

g. IT0017 – Information Technology Incident Response Management

h. IT0102 – Information Technology Asset Management

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

j. IT0506 – Information Technology Account and Credential Management

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

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

m. IT4912 – Information Technology Secure Configuration Management

n. 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/

____