THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0001 - General Statement on Information Technology Policy	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy establishes the University's general cybersecurity framework, roles and responsibilities for university constituents as they relate to information technology policies and procedures, the University's rights, and definitions for terms used throughout System-wide information technology policies.

II. Information Security Program & Cybersecurity Framework

The University will develop, adopt, and adhere to an IT Security Program Strategy (reference the System-wide Policy: IT0003 - Information Technology Security Program Strategy for more information) which demonstrates compliance with this policy. The IT Security Program Strategy is the responsibility of the University of Tennessee System Chief Information Security Officer (CISO). More stringent requirements may be applied than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy based on approval from the University of Tennessee System Chief Information Officer (CIO).

The University has chosen to adopt the principles established in the Center for Internet Security (CIS) Critical Security Controls® (CSC) and all University information technology policies are based on those principles. The strength in the CIS CSC is that it provides a structure that is conducive to the University's current business model, and it can be mapped to multiple compliance frameworks, including but not limited to, the National Institute of Standards (NIST) Cyber Security Framework (CSF), the NIST SP 800-171 controls, PCI version 3.2.1 and 4, and the Service Organization Control 2 used for cloud services.

III. Roles and Responsibilities

1. University of Tennessee System Chief Information Officer (CIO)

a. The University of Tennessee System CIO is the University CIO.

b. The University CIO the only University position approved for the creation and revision of system-wide information Technology policies.

c. The University CIO is responsible for:

i. Designating a University of Tennessee System Chief Information Security Officer (CISO).

ii. Coordinating with the University of Tennessee System CISO to ensure that the University develops and maintains a sound Information Technology (IT) Security Program Strategy and that all the University's IT Resources (Resources) adhere to the controls as defined in the program.

iii. Granting exceptions to policy.

2. Campus or Institute Chief Information Officer (CIO)/Designated Technology Leader (DTL)

a. The campus or institute CIO/DTL is the most senior information technology leader for the campus or institute as designated by the campus or institute's most senior executive leader.

b. The campus or institute CIO/DTL is responsible for:

i. Managing all risks associated with University Information Technology Assets (Assets) , Systems, and Resources under their campus or institute's purview.

ii. Identifying a Chief Information Security Officer (CISO) or Designated Information Security Leader (DISL) for their respective campus or entity.

iii. Granting exceptions to campus or institute processes and procedures.

3. University of Tennessee System Chief Information Security Officer (CISO)

a. The University of Tennessee System CISO is the University CISO.

b. The University CISO is responsible for:

i. Establishing a Security Community of Practice (SCoP) that will consist of the Chief Information Security Officers (CISO) or Designated Information Security Leaders (DISL) and/or other information security subject matter experts from each University campus/institute.

ii. Establishing a governance, risk, and compliance (GRC) program for the University system.

iii. Enforcing the implementation of system-wide information technology policies.

4. Campus or Institute Chief Information Security Officer (CISO)/Designated Information Security Leader (DISL)

a. The campus or institute CISO/DISL is considered the most senior information security expert for the campus/entity as designated by the campus or institute's CIO/DTL.

b. The campus or institute CISO/DISL is responsible for:

i. Developing an Information Technology Security Program Strategy for their respective campus, in accordance with the System-wide Policy: IT0003 – Information Technology Security Program Strategy (hyperlink for more information), that addresses the implementation of the CIS CSC.

ii. Ensuring that the IT Security Program Strategy is adopted, enforced, and reviewed for updates at least annually.

iii. Ensuring that all system-wide Information Technology policies are adhered to.

iv. Ensuring that campus/entity level processes and procedures, in support of each system-wide information technology policy, are developed, communicated, and enforced.

v. Participating in the Security Community of Practice (SCoP) as defined by the University CISO.

5. Security Community of Practice (SCoP)

a. The SCoP is the information security committee that consists of the Chief Information Security Officer (CISO) or Designated Information Security Leader (DISL) and/or other information security subject matter experts from each University campus/institute.

b. The SCoP is responsible for fostering collaboration, sharing knowledge, and enhancing the skills and capabilities of the University in the field of information security including, but not limited to:

i. Knowledge Sharing: Facilitating the exchange of best practices, tools, and strategies related to security (cybersecurity, physical security, etc.) among its campuses.

ii. Promoting Security Awareness: Ensuring that all campuses are educated on the latest security threats and the importance of following security protocols and policies.

iii. Developing Security Standards and Guidelines: Establishing and maintaining security frameworks, standards, and guidelines to ensure consistency and best practices across the organization. The SCoP helps ensure that security practices align with industry standards, regulations, and organizational goals.

iv. Incident Response and Threat Mitigation: Collaborating on handling security incidents and identifying methods for mitigating risks. The SCoP may help in creating incident response plans or provide expertise during a security breach or other incidents.

v. Continuous Improvement: Encouraging ongoing development and refinement of security processes, ensuring that security measures evolve in response to new threats, vulnerabilities, and technological advancements.

vi. Collaboration Across Teams: Working closely with other departments such as IT, compliance, risk management, and operations to ensure a holistic and integrated approach to security across the organization.

vii. Compliance and Risk Management: Ensuring the organization's security practices are in line with legal, regulatory, and compliance requirements. This includes managing risk assessments and audits to identify and address potential vulnerabilities.

6. The Central IT Department

a. The Central IT Department is the System, campus or institute entity responsible for the University's Information Technology Assets (Assets) and Information Technology Systems (Systems) management functions.

b. The Central IT Department is responsible for:

i. Informing all Users of their responsibilities in the use of any of the University's Assets or Systems assigned to them.

ii. Providing training and guidance to the campus or institute community on any process or procedure that was created to support the implementation of an IT security control.

7. Users

a. Users include but are not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's Information Technology Assets, Systems, Resources, and Data.

b. All Users of the University's Assets, Systems, Resources, and/or Data are responsible for:

i. Being familiar with, and complying with, the most recent versions of all University policies.

ii. Being familiar with, and complying with, the most recent versions of all associated campus/entity information security processes and procedures.

iii. Protecting the University's Data based on regulatory, contractual, or University policy, regardless of where it is stored.

iv. Coordinating with the Data Owner and/or Data Steward to gain access to the Data under the Data Owner's purview.

v. Accepting the University's Acceptable Use Policy

c. The University will consider a User to have accepted the University's IT policies and procedures if a User accesses, uses, or handles the University's Assets, Systems, Resources, or Data.

d. All Users will not use a personal Internet account (e.g., Google Mail, Google Storage) for University business.

IV. University Rights

"Data" that is transmitted or stored on the university's Resources is the property of the University unless it is specifically identified in writing as the property of other parties. The University reserves the right to access, monitor, review, and release the contents and activity of a User's account(s). The University reserves the right to access any University owned System and any non-University owned System that is or has been connected to the University's Resources or contains University Data. This action may be taken to maintain the integrity of the University's Resources and/or to preserve Protected University Data and the rights of other Users. Additionally, this action may be taken if the security of a System or IT Resource is threatened, misuse of University IT Resources is suspected, or the University has a legitimate business need to review activity or Data. This action will be taken only after obtaining approval from the campus or institute CIO/DTL, an authorized University office (e.g. Office of General Counsel, or Office of Audit and Compliance), or in response to a subpoena or court order.

V. 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

The University is required to establish an appropriate information security program that defines the University's general cybersecurity framework, roles and responsibilities, and information technology policy and procedure development. This policy is the foundation for all additional system-wide information technology policies and standards.

SECTION 3. Scope and Application

This policy applies to all Users of Information Technology Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

SECTION 4. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy could result in adverse human resource actions, up to and including termination. No exceptions to information technology policies or procedures are valid unless the exception is approved as required by this policy.

SECTION 5. Definitions

Availability – Ensures timely and reliable access to and use of information by authorized users.

Central IT Department – The System, campus or institute entity responsible for the University's Information Technology Assets (Asset) and Information Technology Systems (System) management functions.

Confidentiality – Ensures that the Data is protected from unauthorized access and/or disclosure.

Cybersecurity Framework – A set of standards, guidelines, and practices that an organization leverages to protect against cyber threats.

Data – A collection of facts, information, and statistics that can be in various forms such as numbers, text, sound, images, or any other format. Data can be electronic or physical.

Data Confidentiality Categorization – The categorization given to Data based on the importance of maintaining the confidentiality of the Data.

Data Custodian – The person or unit responsible for implementing controls the Data Owner identifies. This role often includes support from the Central IT Department or departmental technology support.

Data Flows – Defines and documents what, how, and when Data transverses in and out of a University System. This includes direct connections that share Data and indirect connections, like file storage, that provide mechanisms for Data to move between Systems electronically.

Data Integrity Categorization – The categorization given to Data based on the importance of maintaining the integrity of the Data.

Data Owner – The individual or group who has accountability and authority to make decisions about a specific set of Data. The Data Owner is responsible for the function or functions that collect and use the Data, determines the levels of protection for the Data, makes decisions on appropriate use of the Data, and determines the appropriate categorization (reference System-wide Policy: IT0005 - Data Categorization for more information on Data categorization) of the Data. This role generally falls to a functional administrative or academic area, such as the Registrar, Human Resources, the offices of the Chief Financial Officer, Chief Business officer, or Provost, for University Data. This role is not assigned to individual contributors, primary investigators, or other non-executive positions, and is not a role UT is assigned for third party Data in use by the University.

Data Steward – The person who is identified by the Data Owner to act, and to approve or deny access to Data, on behalf of the Data Owner.

Data User – Any person who interacts with the Data. This includes people or programs that create, update, read, or delete information.

Incident Manager – The individual responsible for overseeing the process of responding to and managing security incidents for the campus. This individual is designated by the campus CIO/DTL.

Information Technology Asset (Asset) – As defined in the CIS Critical Security Controls®, includes all end-user devices, IT Network devices, non-computing/Internet of Things (IoT) devices, and servers that exist in virtual, cloud-based, or physical environments, including those that can be connected to remotely. For University policy, Information Technology Assets are defined as those that are owned and managed by the University and that have the potential to store, process, or transmit Data. Included in this definition is the Software Asset which is the programs and other operating System information used within an Information Technology Asset.

Types of Information Technology Assets include, but are not limited to:

- End-user devices, such as desktops, workstations, laptops, tablets, and smartphones.
- IT Network devices, such as wireless access points, switches, firewalls, physical/virtual gateways, and routers.
- Non-computing/Internet of Things (IoT) devices, such as Industrial Control Systems (ICS), smart screens, printers, physical security sensors, and IT security sensors.
- Servers, such as web servers, email servers, application servers, and file servers.

Types of software Assets include, but are not limited to:

- Operating Systems.
- Web applications.
- Database applications.
- Cloud-based applications.
- Mobile applications.

Information Technology Asset Custodian – The User responsible for identifying and documenting the Asset types used for University business.

Information Technology Network – Refers to the interconnected System of hardware, software, and communication protocols that facilitate the transmission, sharing, and storage of Data within the University community. This includes all the infrastructure and services that support digital communication and information management across campus. Key components of a University's IT Network typically include:

- **Local Area Networks (LANs):** These connect computers and devices within specific buildings or areas on campus.
- **Wide Area Networks (WANs):** These link multiple LANs across different locations, potentially including off-campus sites.
- **Wireless Networks (Wi-Fi):** Provides wireless internet access to students, faculty, staff, and visitors throughout the campus.
- **Internet Connectivity:** High-speed connections to external internet service providers (ISPs) for global internet access.
- **Data Centers:** Centralized facilities housing servers, storage Systems, and networking equipment to manage critical applications and Data.
- **Virtual Private Networks (VPNs):** Secure remote access solutions allowing users to connect to the University's network from off-campus locations securely.
- **Firewalls and Security Systems:** Tools used to protect the IT Network from unauthorized access and cyber threats.

Information Technology Security Program Strategy – Includes the procedures and guidance information that defines the implementation strategies and steps for compliance with the Center for Internet Security (CIS) Critical Security Controls (CSC) Implementation Group 1 (IG1) at a minimum and implementation strategies and steps for compliance with the CIS CSC Implementation Group 2 and Implementation Group 3. Includes the implementation strategies and steps for compliance with other security frameworks as needed per contractual requirements and identifies and assigns the security responsibilities including who is responsible for evaluating and accepting risk at each campus and institute.

Information Technology Service Provider – A third-party (non-University funded) individual or entity that provides a variety of IT services and solutions to the University to create, manage, or deliver data and support business functions as needed. The services may include IT management, cloud solutions, software development, cybersecurity, systems integration, storage, and digital transformational support.

Information Technology Resource (Resource) – Information Technology Resource is a broader term for all things related to information technology from a holistic point of view and covers all University owned or managed information technology services, including cloud-based services, that Users have access to. Examples include:

- The IT Network as a single entity.
- The virtual machine cluster.
- The Microsoft Office 365 instance.
- The research enclave.

Information Technology System (System) – A discrete set of information technology Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Data. A System is defined based on functionality, a specific process, or specific duty more so than a specific hardware or software solution. Examples of a System include:

- A cloud application for a department, unit, or the University.
- An on-premises collection of hardware and software designed for a specific research task.
- A control System designed for a specific mission (HVAC, electrical, security).
- A subset of computers in a department specifically designated to meet the business processes of the department.

Integrity – Ensures that Data is protected from unauthorized change and/or manipulation.

Personally Identifiable Information (PII)

Per Tennessee Code Annotated § 47-18-2107, is defined as:

(4) “Personal information”:

(A) Means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements:

(i) Social security number;

(ii) Driver license number; or

(iii) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

(B) Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.

Protected University Data – Data that is protected against unwarranted disclosure. Protection may be required for legal, ethical, privacy, or proprietary considerations. This includes any Data categorized per System-wide Policy: IT0005 – Data Categorization as Internal Use Only (Level 1), Private (Level 2), or Restricted (Level 3) for confidentiality. Examples of Protected University Data include:

- Employee performance reviews.
- Tennessee Unique ID.
- Payment Card Industry (PCI) Data.
- Family Educational Rights and Privacy Act (FERPA).
- Protected Health Information (PHI) per the Health Insurance Portability and Accountability Act (HIPAA).
- Gramm–Leach–Bliley Act (GLBA) Title IV loan Data.
- Personally Identifiable Information (PII).
- Controlled Unclassified Information (CUI).
- Export-Controlled Information (ITAR, EAR).
- Export Administration Regulation (EAR99).
- Sensitive Identifiable Human Subject Research Information (Human Subject).

Risk Assessment – A comprehensive project that evaluates the potential for harm to occur within a scope of information Assets, controls, and threats.

Risk Management – A process for analyzing, mitigating, overseeing, and reducing risk.

Safeguard Maturity – A score of '1' through '5' designating the reliability of a Center for Internet Security (CIS) Safeguard's effectiveness against threats.

Security Event - Any observable occurrence in a System or IT Network that requires investigation and review because it is suspected of being an incident.

Security Incident – Is an event that compromises the confidentiality, integrity, or availability of an information System, IT Network, or Data. This can include unauthorized access to Systems or Data, theft or loss of sensitive information, disruption of service (such as through a denial-of-service attack), or any other activity that poses a threat to organizational Assets.

Unit – An operational entity such as a Campus, Institute, division, or department.

University Data – Any information, Data, or records that are created, gathered, analyzed, or published by any unit or User for the University of Tennessee in support of its mission(s).

University Employee (Employee) – An individual who works for a University in any capacity, including academic, administrative, technical, and support roles. University Employees can be categorized into several types based on their functions and employment status:

- Faculty: These are academic staff members such as professors, lecturers, and researchers responsible for teaching and conducting research.
- Administrative Staff: Individuals involved in the management and administration of University operations. This includes roles like deans, department heads, registrars, and HR personnel.
- Technical Staff: Employees who manage and maintain the University's IT infrastructure, laboratories, and other technical facilities.
- Support Staff: Workers providing essential services such as maintenance, security, custodial work, dining services, and student support.
- Student Employees: Any student who is compensated by the University in an official capacity for a service.

User Account – Includes the following:

- Standard user accounts: These are the most common type of user account associated with your primary affiliation, such as being a student or an Employee, with the University and are used for everyday tasks like running software or personalizing your desktop.

- Privileged accounts: These accounts have full access to all settings on a System and are used for making changes to System settings or managing other accounts.
- Guest accounts: These accounts are used by temporary or intermittent users of a computer. They allow users to log in without making changes to the System's settings or accessing other users' folders.
- System accounts: These accounts are used for storing System files and processes.
- Root accounts: These accounts are used for System administration.
- Database accounts: These accounts are used for database access.
- Service accounts: A special type of account used to enable automated processes or applications to interact with various services or Systems without requiring user intervention.

Users – Includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's Information Technology Assets, Systems, Resources, and Data.

Vulnerability Management – Monitoring of vulnerability announcements and emerging threats applicable to the University's Assets, Systems, and Resources that includes establishing clear lines of communication regarding threat intelligence between the vendor(s) and the University.

____

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 IT Resources if an individual violates this policy.

____

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number (xxx) xxx-xxxx	Email/Web Address
Policy Clarification and Interpretation	System Chief Information	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu

	Officer and System Chief Information Security Officer		
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[Text Wrapping Break]____

SECTION 8. Policy History

Revision 1:

____

SECTION 9. Related Policies/Guidance Documents

A. **University Policies**

a. IT0002 – Acceptable Use of Information Technology Resources

b. IT0003 – Information Technology Security Program Strategy

c. IT0004 – Information Technology Risk Management

d. IT0005 – Data Categorization

e. IT0014 – Security Awareness Training Management

f. IT0017 – Information Technology Incident Response Management

g. IT0102 – Information Technology Asset Management

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

i. IT0506 – Information Technology Account and Credential Management

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing

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

l. IT4912 – Information Technology Secure Configuration Management

m. 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/

____