System-wide Policy: IT0002 - Acceptable Use of Information Technology Resources	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy establishes the guidelines and expectations for the acceptable use of the University's Information Technology Assets, Systems, Resources, and Data.

II. Privacy Notice for Users

1. Users have no expectation of privacy when using University IT Resources.

a. As required by state law, the University hereby notifies Users that University Data, regardless of where it is stored, including email, may be subject to and open to public inspection under Tennessee's open-records laws, including without limitation the Tennessee Public Records Act, unless applicable laws deem a particular record confidential. More information can be found here: https://communications.tennessee.edu/public-records/. Further, the University hereby notifies Users that University Data might be disclosed in the event of a court order, such as a subpoena.

b. Any activity on the University's Resources may be monitored, logged, and reviewed by University-approved personnel or may be discovered in legal proceedings. All Data created, stored, transmitted, or received on the University's Resources may be subject to monitoring by System administrators.

2. The University may share information, including certain personally identifiable information (PII), with its vendors performing institutional services or functions for the purpose of utilizing single sign-on (SSO), as permitted by FERPA or other applicable regulations.

III. 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 Chief Information Officer (CIO)/Designated Technology Leader (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. 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.

IV. User Responsibilities

Each User of the University's Assets, Systems, Resources, or Data is required to be familiar and comply with University policies. Each User is required to protect the University's Data based on the requirements in this policy regardless of where it is stored. Data Users are responsible for contacting the Data Owner and/or Data Steward to gain access to the Data.

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. Users are responsible for ensuring that they are familiar with the latest versions of the University's policies.

1. All Users of the University's Resources must:

a. Familiarize themselves with, and comply with, all University policies and campus or institute processes and procedures to secure University Data.

b. Only use the University's Resources for which the User has authorization. This behavior includes using only the passwords and the privileges associated with their System account(s) and the use of those account(s) only for their authorized purpose.

c. Be responsible for using University-approved Resources for University Data and understanding the back up and retention policies associated with the University's Resources.

d. Properly log out of sessions when no longer in use.

e. Monitor access to their accounts. If a User suspects unauthorized activity or their University-managed account has been compromised, they must report the compromise per the Central IT Department's defined process.

f. Respect and honor the rights of other individuals regarding intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of the University's Resources.

g. Transmit Protected University Data externally using only an approved method such as Secure FTP or encrypted e-mail. If secure transmission is needed, contact the Central IT Department

h. Enable multi-factor authentication (MFA) for access to all University Systems and applications that store, process, or transmit Protected University Data including cloud-based applications and services.

2. All Users while using a University-owned IT Asset must:

a. Use only approved, supported, and patched applications and operating systems on University-owned Systems. Contact the Central IT Department for more information.

b. Work with the Central IT Department to ensure that any University-owned desktop, laptop, tablet, or phone is encrypted when traveling outside the United States except for travel to locations as described below in section 4.

c. Contact their IT Support office for a loaner device when traveling to a locations outside of the United States as described below in section 4.

d. Use software that has been approved by the Central IT Department for University Systems. Reference the System-wide Policy IT0102 - Information Technology Asset Management for more information.

e. Use University provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous Users, and other terms of the license.

3. All Users of the University's Resources must not:

a. Share University-assigned authentication credentials to the University's Resources.

b. Use accounts, access codes, privileges, or the University Resources for which they are not authorized.

c. Attempt to circumvent the security controls and/or configurations of the University's IT Assets, Systems, or Resources.

d. Tamper, modify, or alter any restrictions or protections placed on their accounts, or the University's Resources.

e. Vandalize or intentionally physically damage the University's IT Assets, Systems, or Resources.

f. Use the University's Resources to introduce, create, or propagate malicious email such as spam or phishing, computer viruses, worms, trojan horses, or other malicious code.

g. Eavesdrop on or intercept other Users' transmissions.

h. Attempt to degrade the performance or availability of any System or to deprive authorized Users access to the University's Resources. This behavior includes using any device or application that consumes a disproportionate amount of IT Network bandwidth without prior authorization from the Central IT Department.

i. Intentionally misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering on the University's Resources.

j. Send email mass mailings for purposes other than official University business.

k. Use University Resources as an email relay between non-University email Systems (routing email through University email Systems between two non-University Systems).

l. Engage in activities that violate state or federal law, a University contractual obligation, or another University policy or rule including but not limited to Human Resources policies and Standards of Conduct for students.

m. Comment or act on behalf of the University over the internet without authorization.

n. Connect devices (such as switches, routers, hubs, Systems, and wireless access points) to the IT Network without prior approval from the campus or institute IT organization.

o. Include or request Protected University Data be included in unprotected electronic communication (email, instant message, text message, etc.).

p. Attempt to gain access to the University's Resources without authorization from the Central IT Department.

q. Use personally licensed internet services (e.g., Google Mail, Google storage) for University business or store University Data on a personally owned System or device.

4. All Users while using a University-owned IT Asset must not:

a. Take their assigned University desktop, laptop, tablet, phone or device when traveling outside the U.S. to:

i. A foreign county of concern as defined by 42 U.S.C. § 19237 located here: https://www.law.cornell.edu/uscode/text/42/19237; or

ii. A foreign country that is the subject of a sanctions program maintained by the Office of Foreign Assets Controls (list available here: https://ofac.treasury.gov/sanctions-programs-and-country-information); or

iii. A foreign country that is the subject of a Department of State Arms Embargo as identified in ITAR § 126.1 (list available here:

https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_country_landing); or

iv. A foreign country that is the subject of EAR Part 746 Embargoes (list available here: https://www.bis.doc.gov/index.php/documents/regulation-docs/420-part-746-embargoes-and-other-special-controls/file).

b. Transport Protected University Data out of the United States on Systems without approval from the University CIO.

V. Copyrights and Licenses

1. Violation of copyright law or infringement is prohibited by University policy and federal law, including with respect to the use of the University's Assets, software or Data. Any unauthorized use of copyrighted material 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 Campus Code of Conduct or the Human Resources Policy and Procedures.

2. Copied material used with the University's Resources or Data must be properly credited using applicable legal and professional standards.

3. Software may not be copied, installed, or used on the University's Resources except as permitted by the owner of the software and by law.

4. When using the University's Resources, Users will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous Users, and terms of the license.

5. All copyrighted information, such as text and images, retrieved from the University's Resources or stored, transmitted, accessed, or maintained with the University's Resources must be used in compliance with applicable laws.

6. Each University Unit is responsible and accountable for maintaining records of purchased software licensure on the University's Assets and Systems. The providing organization is responsible for

maintaining records and information related to centrally provided software. These records are subject to internal or external audit for compliance.

7. This policy does not affect Fair Use provisions in federal copyright law.

VI. Personal Use

1. The University's Resources are provided for use in conducting authorized University business. All Users are prohibited from using the University's Resources for personal gain, illegal activities, or obscene activities.

2. The prohibition against using the University's Resources for personal gain does not apply to:

a. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members.

b. Consulting and other activities that relate to an employee's professional development or as permitted under University policy.

3. The University allows incidental or casual personal use of the University's Resources, except when such use:

a. Is excessive or interferes with the performance of the User's University responsibilities.

b. Results in additional incremental cost or burden to the University's Resources.

c. Violates any state or federal law or is otherwise in violation of University policies and procedures, including campus procedures.

d. Results in additional material risk to the security of the University's Resources.

4. The University's Resources may not be used for commercial purposes, except as specifically permitted under written University policy or with the written approval of the General Counsel's office.

5. Any commercial use of the University's Resources must be properly related to University activities and provide for appropriate reimbursement of taxes and other costs the University may incur by reason of such use.

6. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use. Activities not appropriate for the ".edu" domain but otherwise permissible using the University's Resources must use other domain designations.

7. The University accepts no responsibility to maintain or secure Data related to personal use that a User chooses to store on the University's Resources. The User accepts all risks associated with personal use.

VII. Misuse of the University's Resources

1. Any violation of User Responsibilities will be considered a misuse of the University's Resources.

2. Users must report all suspected or observed illegal activities to the appropriate University or campus or institute administrative office. Examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.

3. Abuse of the University's Resources, regardless of location, will be treated as an abuse of Resource privileges.

4. State law prohibits the use of the University's Resources by University Employees (Employee) for campaign or political advertising on behalf of any party, committee, agency, or candidate for political office. (Tennessee Code Annotated § 2-19-201 et seq.). This does not prohibit use of the University's Resources to discuss or examine political topics or issues of public interest, so long as it does not advocate for or against a particular party, committee, agency, or candidate. For more information, review General Policy: GE0003 - State and Federal Government Relations Activities.

VIII. 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 guidelines and expectations for the acceptable use of the University's Information Technology Assets, Systems, Resources, and Data 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 University Information Technology 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 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 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 3: 10/1/2017

Revision 4: TBD

_____

SECTION 9. Related Policies/Guidance Documents

A. **University Policies**

a. IT0001 – General Statement on Information Technology Policy

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/
