THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0110 - Acceptable Use of Information Technology Resources	
Version: 3	**Effective Date: 01/13/2016**

IT0110 - Acceptable Use of Information Technology Resources

Objective:

This document establishes policy for the acceptable use of information technology resources at the University of Tennessee. The University community is based on principles of honesty, academic integrity, respect for others, and respect for others' privacy and property; thus, The University seeks to:

1. Protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under federal and state law, including the Tennessee Open Records Act;
2. Ensure that the use of electronic communications complies with the provisions of University policy and state and federal law; and
3. Allow for the free exchange of ideas and support of academic freedom.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee System including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

System-wide Policy: IT0110 - Acceptable Use of Information Technology Resources	
Version: 3	**Effective Date: 01/13/2016**

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The individual or position should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program which demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements 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.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

Policy:

1. **User Privacy**
    a. There should be no expectation of privacy on the part of the User.
    b. As required by state law, the University hereby notifies users that email may be a public record and open to public inspection under the Tennessee Open Records Act, unless the email is covered by an exception to the Act, such as personally identifiable student information, proprietary information, or trade secrets (See UT Information Classification Policy: IT 0115, sections two and three).

c. Users should be aware that any activity on systems and networks may be monitored, logged, and reviewed by university approved personnel or may be discovered in legal proceedings. All documents created, stored, transmitted, or received on university computers and networks may be subject to monitoring by systems administrators.

2. **Users WILL**
   a. Comply with all University policies to ensure confidentiality, integrity, and availability of university resources under their control;
   b. Only use University resources for which the User has authorization;
   c. Be responsible for using University-approved resources for electronic data and understanding the back up and retention policies associated with those resources.
   d. Control and secure physical and network access to University resources, including data;
   e. Properly log out of sessions;
   f. Monitor access to their accounts. If a User suspects unauthorized activity or that their account has been compromised, they must report the compromise to the Campus Authority responsible for information security or their designee, and change passwords immediately;
   g. Install, use, and regularly update virus protection software;
   h. Use only supported and patched applications and operating systems on University-owned devices. Exceptions must be documented and approved by the Campus Authority or their designee.
   i. Where technically possible, abide by the password protection best practices specified for each University resource;
   j. Use only the passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose;
   k. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of University resources;

l. 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. **Users WILL NOT**
   a. Share access codes or passwords;
   b. Use accounts, access codes, privileges or IT resources for which they are not authorized;
   c. Tamper, modify, or alter any restrictions or protections placed on their accounts, the University's system, or network facilities.
   d. Physically damage or vandalize University resources;.
   e. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner;
   f. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious code;
   g. Obtain extra University resources or gain access to accounts for which they are not authorized;
   h. Eavesdrop on or intercept other Users' transmissions;
   i. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any University resources.
   j. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering;
   k. Send email chain letters or mass mailings for purposes other than official University business;
   l. Use University resources as an email relay between non-university email systems (routing email through university email systems between two non-university systems);
   m. 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;

n. Comment or act on behalf of the University over the Internet without authorization.
o. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) to the network without prior approval from the Campus IT organization.
p. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth.
q. Include or request Sensitive Information be included in unprotected electronic communication (email, instant message, text message, etc.).

4. University Rights

a. The University reserves the right to access, monitor, review, and release the contents and activity of an individual User's account(s) as well as that of personal Internet account(s) used for University business. The University reserves the right to access any University owned resources and any non-University owned resources on University property, connected to University networks, or containing University data. This action may be taken to maintain the network's integrity and the rights of other authorized Users. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of University 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 Authority, 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.

5. Copyrights and Licenses

a. Violation of copyright law or infringement is prohibited by University policy and state and federal law. 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 Code of Conduct in the Human Resources Policy and Procedures;

b. Software may not be copied, installed, or used on University resources except as permitted by the owner of the software and by law;
c. 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;
d. All copyrighted information, such as text and images, retrieved from University resources or stored, transmitted, accessed, or maintained with University resources must be used in compliance with applicable copyright and other laws;
e. Copied material must be properly credited using applicable legal and professional standards;
f. Each Unit is responsible and accountable for maintaining records of purchased software licensure. The providing organization is responsible for maintaining records and information related to centrally provided software. These records are subject to internal audit for compliance

6. Personal Use

a. University Resources are provided for use in conducting authorized University business. All users are prohibited from using these resources for personal gain, illegal activities, or obscene activities.
b. The prohibition against using the University's IT resources for personal gain does not apply to:
    i. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members;
    ii. Consulting and other activities that relate to a faculty member's professional development or as permitted under University policy;
c. Incidental or casual personal use of these resources is permitted by this policy, except when such use:
    i. Is excessive or interferes with the performance of the User's University responsibilities.
    ii. Results in additional incremental cost or burden to the University's resources;

iii. Violates any state or federal law or is otherwise in violation of this or any other University policy;

iv. Results in additional risk to the confidentiality, integrity, and availability to the University's resources.

d. University IT resources may not be used for commercial purposes, except as specifically permitted under other written university policies or with the written approval of the Campus Authority.

e. Any commercial use of University IT 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.

f. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use;

g. Activities not appropriate for the ".edu" domain but otherwise permissible using University resources must use other domain designations.

h. University Campuses may impose more stringent restrictions on personal use.

7. Misuse of IT Resources

a. Users must report all suspected or observed illegal activities to the appropriate University or Campus 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.

b. Abuse of networks or computers at other sites through the use of University resources will be treated as an abuse of resource privileges.

c. State law prohibits the use of University resources by employees 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 University 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.

References: n/a

Definitions:

1. **Unit** - An operational entity such as a Campus, Institute, division, or department.
2. **Sensitive Information** - Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies.

Last Reviewed: January 13, 2016