UTIA IT0110 – Acceptable Use Of Information Technology Resources Security Plan (AUP)

Effective: May 22, 2018
Last Reviewed: March 20, 2018 **Last Updated:** May 17, 2018

Objective:
This plan is based on NIST Special Publication 800-53, as well as UT Policy IT0110 – *Acceptable Use of Information Technology Resources*, and defines guidelines for the University of Tennessee Institute of Agriculture (the Institute) and its IT assets. Users are required to review this plan at least annually, as well as have an understanding of and full compliance with the plan.

Scope:
This plan applies to IT assets owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users who access, use, or handle the Institute's IT assets. IT assets include, but are not limited to all Institute-owned desktops, laptops, servers, devices, telephones, and networks (institute- and University-owned). This plan also applies to the use of all University IT resources.

Plan:

1. **User Privacy**
   a. Users should have no expectation of privacy when using Institute-owned IT assets.
   b. As required by state laws, email may be considered a public record, therefore open to public inspections under the Tennessee Open Records Act, unless covered under exception to the Act (i.e., personally identifiable student information, proprietary information, or trade secrets).
   c. Users should be aware that any activity on Institute-owned IT assets, including telephones, may be monitored, logged, and reviewed by approved personnel, and may be discovered in legal proceedings. All data created, stored, transmitted, or received using Institute-owned IT assets are subject to monitoring by approved personnel.

2. **Users WILL**
   a. Comply with all Institute policies (also called plans) and procedures, as well as all University policies, to ensure confidentiality, integrity, and availability of Institute-owned IT assets under their control.
      - Regularly review all policies and procedures.
      - Use of Institute-owned IT assets implies acceptance of this plan.

b. Use only Institute-owned IT assets for which explicit authorization has been given.
   - If you need access to additional Institute-owned IT assets, ask your supervisor.
   - If you no longer need access to an Institute-owned IT asset, tell your supervisor.
   - Refer to UTIA IT0130 – *Personnel Security Plan for Information Technology* and UTIA IT0132 – *Identification and Authentication Plan*.
c. Be responsible for using Institute-owned IT assets and understand the associated backup and retention policies and best practices.
   - Back up your data properly and regularly.
   - Refer to UTIA IT01xx – *Media Protection Plan* for retention and disposal of Institute-owned IT assets.
d. Control and secure physical and network access to Institute-owned IT assets, including data.
   - Refer to UTIA IT0120 – *Secure Network Infrastructure Plan*, UTIA IT0120P – *Secure Network Infrastructure Procedures*.
e. Properly log out of sessions and devices.
   - Refer to UTIA IT01xx – *Information Technology Access Control*, UTIA IT0129 – *Physical and Environmental Protection Plan*, and UTIA IT0129P – *Physical and Environmental Protection Procedures.*
f. Monitor access to their accounts.
   - If a user suspects unauthorized activity on their account(s) or that their account(s) has been compromised, that user must report to the Institute's Chief Information Security Officer (CISO), and change password(s) immediately using a different device.
   - Refer to UTIA IT0122 – *Information Security Incident Response Plan* and UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*.
g. Install, use, and regularly update virus protection and malware protection software.
   - Refer to UTIA IT0135 – *System and Information Integrity Plan*
h. Use only supported and patched applications and operating systems on Institute-owned devices.
   - Refer to UTIA IT0125 – *Information Technology Configuration Management Plan*.
i. Abide by password protection best practices and policies for all Institute-owned IT assets.
   - Refer to UTIA IT0132 – *Identification and Authentication Plan*.
j. Use only credentials (user names and passwords) associated with their computer account(s) and only for their authorized purpose.
   - Refer to UTIA IT0132 – *Identification and Authentication Plan*.
k. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of Institute-owned IT assets.
   - Refer to HR0508 – *Code of Conduct*.
l. Use Institute- and 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 licensing agreement.

- Refer to UT Knoxville Office of Information Technology's (OIT) Software Procurement, Distribution, and Licensing and UT Policy FI0130 – *Fraud, Waste, and Abuse*.

3. Users WILL NOT

a. Share access codes or passwords.
   - Never ask others for their passwords.
   - Never give anyone your password.
   - Shared accounts must be requested through the appropriate channel and only when there is a valid reason.
   - Refer to UTIA IT0132 – *Identification and Authentication Plan*.

b. Use accounts, access codes, privileges, or Institute-owned IT assets for when they are not authorized.
   - Refer to UTIA IT01xx – *Information Technology Access Control Plan* and UTIA IT0132 – *Identification and Authentication Plan*.

c. Tamper with, modify, or alter any restrictions or protections placed on their accounts, Institute-owned IT assets; the University's system, or network facilities;
   - Refer to UTIA IT0129 – *Physical and Environmental Protection Plan* and UTIA IT0120 – *Secure Network Infrastructure Plan* and UT Policy FI0130 – *Fraud, Waste, and Abuse*.

d. Physically damage or vandalize Institute-owned IT assets.
   - Refer to UT Policy FI0130 – *Fraud, Waste, and Abuse*.

e. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner.
   - Refer to UT Office of General Counsel's Copyright Information and *Copyright Law of the United States*.

f. Use Institute-owned IT assets to introduce, create, or propagate spam, phishing email, computer viruses, worms, Trojan horses, or other malicious code.
   - Refer to OIT's Spam Policy.

g. Obtain extra Institute-owned IT assets or gain access to accounts for which they are not authorized.
   - Refer to UTIA IT01xx – *System and Services Acquisition Plan* and UTIA IT0132 – *Identification and Authentication Plan*.

h. Eavesdrop on or intercept other Users' transmissions;
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

i. Attempt to degrade the performance or availability of any system or to deprive authorized Users' access to any Institute-owned IT assets or University resources.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

j. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

k. Send email chain letters or mass mailing for purposes other than official business;
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

l. Use Institute-owned IT assets as an email relay between non-university email systems.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

m. Engage in activities that violate Institute policies, plans, or procedures; local, state, or federal law, an Institute or University contractual obligation, or other University policy or rule including but not limited to Human Resources policies and Standards of Conduct for students.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

n. Comment or act on behalf of the Institute or University over the Internet without proper authorization.

o. Connect devices (i.e., switches, routers, hubs, computer systems, wireless access points) to the network without prior approval from the Institute's Chief Information Officer (CIO).
   - Refer to UTIA IT0120 – *Secure Network Infrastructure Plan* and OIT's wireless network policies.

p. Use without authorization any device or applications that consumes a disproportionate amount of network bandwidth.
   - Refer to UTIA IT0120 – *Secure Network Infrastructure Plan*.

q. Include or request sensitive information be included in non-secure electronic communication, such as email, instant message, text message, Skype conversations, Zoom meetings, etc.

4. Institute and University Rights

The Institute and the University reserve 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 Institute business. The Institute and University reserve the right to access any Institute-owned IT assets, University-owned resources, and any non-University-owned resources on Institute or University property, connected to Institute or University networks, or containing Institute or 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 Institute-owned IT assets or University resources is suspected, or the Institute or University has a legitimate business need to review activity or data. This action will be taken only after obtaining approval from the Institute's Chief Information Security Officer; Human Resources; Office of General Counsel; Office of Audit and Compliance; campus, local, state, or federal law enforcement; 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 Code of Conduct* or to discipline under the HR0580 – *Code of Conduct*.

b. Software may not be copied, installed, or used on Institute-owned IT assets or University resources except as permitted by the owner of the software and by law.

- Refer to UT Office of General Counsel's Copyright Information and *Copyright Law of the United States*.

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.
   - Refer to UT Knoxville Office of Information Technology's (OIT) Software Procurement, Distribution, and Licensing.

d. All copyrighted information, such as text and images, retrieved from Institute-owned IT assets; University resources; or stored, transmitted, accessed, or maintained with Institute-owned IT assets or University resources must be used in compliance with applicable copyright and other laws.
   - Refer to UT Office of General Counsel's Copyright Information and *Copyright Law of the United States*.

e. Copied material must be properly credited using applicable legal and professional standards.
   - Refer to UT Office of General Counsel's Copyright Information and *Copyright Law of the United States*.

f. The Institute 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.
   - Refer to UT Office of General Counsel's Copyright Information and *Copyright Law of the United States*.

6. Personal Use

a. Institute-owned IT assets are provided for use in conducting authorized Institute business. All users are prohibited from using these resources for personal gain, illegal activities, or obscene activities.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

b. The prohibition against using any Institute-owned IT assets 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 Institute responsibilities;
   ii. Results in additional incremental cost or burden to the Institute;
   iii. Violates any local, state, or federal law or is otherwise in violation of this AUP or any other Institute policy, plan, or procedure; or University policy;

iv. Results in additional risk to the confidentiality, integrity, and availability to and Institute-owned IT assets and data on those assets, as well as the University's resources.

- Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

d. Institute-owned IT assets may not be used for commercial purposes, except as specifically permitted under other written university policies or with the written approval of the appropriate Institute Authority.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

e. Any commercial use of Institute-owned IT assets must be properly related to Institute activities and provide for appropriate reimbursement of taxes and other costs the Institute may incur by reason of such use.
   - Refer to HR0580 – *Code of Conduct* and *Student Code of Conduct*.

f. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use.
   - Refer to the EDUCAUSE .edu Frequently Asked Questions.

g. Activities not appropriate for the ".edu" domain, but otherwise permissible using Institute-owned IT assets, must use other domain designations.

7. Misuse of IT Assets

a. Users must report all suspected or observed illegal activities to the appropriate 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.
   - Refer to UT Policy FI0130 – *Fraud, Waste, and Abuse*.

b. Abuse of networks or computers at other sites through the use of Institute-owned IT assets or University resources will be treated as an abuse of resource privileges.
   - Refer to UT Policy FI0130 – *Fraud, Waste, and Abuse*.

c. State law prohibits the use of Institute-owned IT assets or University resources by employees for campaign or political advertising on behalf of any party, committee, agency, or candidate for political office per the Little Hatch Act (Tennessee Code Annotated § 2-19-201 et seq.). This does not prohibit use of Institute-owned IT assets to discuss or examine political topics or issues of public interest, so long as such use does not advocate for or against a particular party, committee, agency, or candidate.

References:

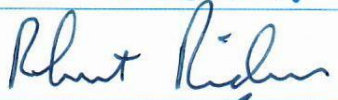
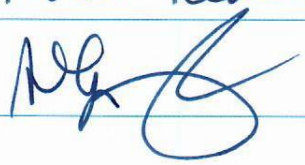
UTIA Glossary of Information Technology Terms
UT Policy IT0110 – *Acceptable Use of Information Technology Resources*
UTIA IT0120 – *Secure Network Infrastructure Plan*
UTIA IT01xx – *Information Technology Access Control Plan*
UTIA IT0129 – Physical and Environmental Protection Plan
UTIA IT0132 – *Identification and Authentication Plan*
UTIA IT0135 – *System and Information Integrity Plan*
UTIA IT01xx – *Media Protection Plan*
UT Policy HR0508 – *Code of Conduct*

Student Code of Conduct
UT Policy FI0130 – *Fraud, Waste, and Abuse*
UT Knoxville OIT Software Procurement, Distribution, and Licensing
UT Knoxville OIT wireless network policies
UT Office of General Counsel's Copyright Information
Copyright Law of the United States
Tennessee Code Annotated § 2-19-201 et seq.
NIST SP 800-53 – *Security and Privacy Controls for Information Systems and Organizations*

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.

Approval of Plan

We approve UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		5/21/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		5/18/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		05/22/2018