UTIA IT01xx – Information Technology Access Control Plan

Effective: September 18, 2017
Last Reviewed: August 18, 2017 **Last Updated:** August 02, 2017

Objective:
The purpose of this plan is to protect the University of Tennessee Institute of Agriculture's (the Institute's) information technology (IT) assets. Access control ensures that an authenticated user accesses only the IT assets and data for which that user is authorized to access.

Scope:
This plan applies to all IT assets and data owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users who access, use, or handle such IT assets or data.

Plan:
The UTIA IT01xx – *Information Technology Access Control Plan* is the official policy and procedures document for IT access control at the Institute. This plan addresses the establishment and implementation of access control policy and procedures. The Institute's Chief Information Security Officer (CISO) is responsible for maintaining the plan, which includes annual review of the plan, and updating as necessary. This plan references other UTIA security plans, which may be found on the UTIA Policies and Procedures website.

The Institute incorporates the following selected security controls from the NIST Access Control family for this plan:

1. Account Management
2. Access Enforcement
3. Least Privilege
4. Unsuccessful Logon Attempts
5. System Use Notification
6. Session Lock
7. Permitted Actions without Identification or Authorization
8. Remote Access
9. Wireless Access

Account Management
The Institute's IT assets are managed by the appropriate IT administrators. The IT administrators will create accounts, both group and role memberships, based on need and will enable, modify, review, disable, and delete accounts accordingly. The accounts are assigned

based on the other security controls specified in this plan. The IT administrators will monitor the use of accounts and will follow the UTIA IT0130 – *Personnel Security Plan for Information Technology* when access needs change or when accounts are no longer needed due to an employee's change in role or termination.

Access Enforcement
Deans, Directors, Department Heads, or other supervisors will approve authorizations for access to the Institute's IT assets and data. Once authorized, the appropriate IT personnel will assign the applicable privileges to Institute and University resources. The CISO will randomly review assigned accesses to ensure the UTIA IT0130 – *Personnel Security Plan for Information Technology* is being followed.

Least Privilege
The Institute will employ the principle of least privilege when assigning access to users. This means that users will be assigned only the minimum rights necessary to perform the roles and responsibilities of the job function. For users who must be assigned administrative access (privileged account), the user will use the non-privileged account when accessing non-security functions. The Institute allows privileged access by third-party providers and any persons outside the Institute (affiliates) based on explicit business justification.

Unsuccessful Logon Attempts
The Institute will enforce, through the baseline configuration for IT assets (UTIA IT0125 – *Information Technology Configuration Management Plan*), a limit of logon attempts by a user. If a user has unsuccessfully attempted to log into the account a specified number of times, the account will be locked for a short duration and the user may try again after that time. This control is in place, in part, to help prevent brute force attacks.

System Use Notification
The Institute's IT assets will be configured to display a screen at login which clearly states that the asset is the property of the Institute and is for authorized use only. The notification informs potential users that the IT asset may be monitored, recorded, and audited, and that use of the IT asset implies consent to monitoring and recording. The text displayed also states that the user acknowledges and agrees with the UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)* and that unauthorized use may be subject to disciplinary action, as well as criminal and civil penalties. The notification will remain on the screen until the user takes action to log onto the IT asset, acknowledging the notification.

Session Lock
The Institute, through the baseline configuration for IT assets, will enforce a session lock as a temporary action taken when a user stops works and the asset is idle. The session lock will be set to initiate a blank screen after a reasonable amount of idle time in order to conceal potentially sensitive data on the screen. The session lock, however, is in no way intended to

take the place of logging out of Institute IT assets, as required in UTIA IT0130 – *Physical and Environmental Protection Plan*.

Permitted Actions without Identification or Authentication

The Institute requires that every action needed to access moderate Institute or University IT assets or other resources must require authentication and the privileges of the user are based on role and responsibilities. Institute and University resources also require authentication and access is assigned using the principle of least privilege. Once logged into an Institute IT asset, public websites may not require additional authentication, but the user is expected to follow the Institute's *AUP*, as well as the University's *AUP*.

Remote Access

The Institute requires that all users with a need to connect to Institute or University IT assets or other resources while not physically located on the UT Knoxville (UTK) network must use the encrypted virtual private network (VPN) to securely connect. This includes all connections using dial-up, broadband, or wireless methods. The use of the VPN protects the confidentiality and integrity of the Institute's data. The VPN solution for those connecting to the UTK network from the statewide locations (i.e., Extension offices, AgResearch Centers, 4-H Centers, regional offices, etc.) is managed and monitored by the Institute's Information Technology Services, while UTK Network Services manages and monitors the VPN solution and software for those working from home or travelling and need access to the Institute's or University's IT resources. Once connected to these resources, the user's normal access privileges are granted.

Wireless Access

The Institute requires that all users connecting to any wireless network must use a secure network when accessing Institute or University IT assets or other resources. This requirement pertains not only to the use of the Institute's or University's WiFi networks, but also to the use of any wireless network when working from home or travelling. The secure wireless network for those connecting to the UTK network from the statewide locations (i.e., Extension offices, AgResearch Centers, 4-H Centers, regional offices, etc.) is managed by the Institute's Information Technology Services and is implemented in accordance with the UTIA IT0120 – *Secure Network Infrastructure Plan*. UTK Network Services manages the secure wireless network for those associated with the Knoxville campus. Using the "guest" network at any location does not allow for privileged access, thus prohibiting access to Institute or UT resources when using a guest network.

References:

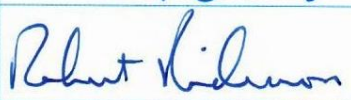
UTIA Glossary of Information Technology Terms
UTIA IT0125 – *Information Technology Configuration Management Plan*
UTIA IT0130 – *Personnel Security Plan for Information Technology*
UTIA IT0130 – *Physical and Environmental Protection Plan*
UTIA IT0120 – *Secure Network Infrastructure Plan*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*

UTIA IT0302 – *Information Technology Formal Exception Plan*
NIST SP 800-53 – *Security and Privacy Controls for Federal 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 the UTIA IT01xx – *Information Technology Access Control Plan* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		9/18/17
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		9/17/2017
Sandra D. Lindsey	Chief Information Security Officer, UTIA		09/14/2017