UTIA IT0130 – Personnel Security Plan for Information Technology

Effective: September 18, 2017
Last Reviewed: July 19, 2017 **Last Updated:** August 09, 2017

Objective:
This plan is to maintain a program for Personnel Security, addressing the need to ensure individuals granted access to certain University of Tennessee Institute of Agriculture (the Institute) IT assets and data have been properly vetted. This plan is consistent with University requirements, as well as applicable regulations, guidelines, and local, state, and federal laws.

Scope:
This plan and its procedures apply to all Institute employees, which includes administration, staff, contractors, and student employees, as well as any persons outside the Institute (affiliates) and third-party providers who have a legitimate and approved business need to access Institute IT assets or data classified as moderate, high, or business critical.

Procedures:
Personnel Screening
All employees, affiliates, and third-party providers will be subjected to a background check prior to gaining access to the Institute's IT assets and/or data classified as moderate, high, or business critical. This screening is a part of the UT System Human Resources Pre-Employment Background Checks, with the guidelines found at https://hr.tennessee.edu/jobs/background-checks/.

The appropriate Dean, Director, or Department Head is responsible for ensuring that affiliates, who carry out Institute business functions, have met all personnel screening requirements. This includes, but is not limited to, Tennessee State University (TSU) employees, fully-funded county employees, seasonal workers, externs, or volunteers.

Personnel screening requirements for third-party providers must be explicitly stated in any acquisition-related documents. Third-party providers are expected to comply with all established and documented security requirements and will be monitored.

Personnel Termination
Institute Employees:
Immediately upon termination of employment, the Institute employee will:

1. Take part in the checkout process, which will include a discussion with the supervisor of any access to IT assets or media.
2. Return all IT assets and media owned by the Institute, including all IT assets that have been checked out for use outside the office.

Immediately upon termination of employment, the supervisor will:

1. Contact the local/regional IT representative or the Institute's Chief Information Security Officer (CISO) to report the termination and inform of all known access to IT assets or media.
2. Contact the OIT HelpDesk to have the IT assets reformatted and the operating system reinstalled.

Immediately upon termination of employment, the CISO (or local/regional IT representative, where applicable) will:

1. Remove any IT assets used by the employee from the University's network registration database. If the IT asset should not be removed from the network, ownership will be temporarily reassigned.
2. Contact the appropriate persons for revoking credentials associated with the terminated employee.

Affiliates and Third-Party Providers:

Immediately upon termination of specified work, the appropriate Dean, Department Head, or Director responsible for the affiliate or third-party provider will notify the UTIA CISO (or local/regional IT representative, where applicable). The CISO or local/regional IT representative will:

1. Remove any IT assets used by the affiliate or third-party provider from the University's network registration database.
2. Contact the appropriate persons for revoking credentials associated with the affiliate or third-party provider.

Personnel Transfers

Any employee leaving an Institute department and transferring to another department within the Institute or to another department outside the Institute, but within the University system, will retain access to his/her employee-assigned storage, as well as the NetID credentials.

When an Institute employee transfers to another department within the Institute, the supervisor will:

1. Contact the local/regional IT representative or OIT HelpDesk to assist the employee with moving departmental data from the employee's assigned storage areas to a departmental storage area with the appropriate controls in place for least privilege access. (see UTIA IT01xx – *Information Technology Access Control Plan*).
2. Contact the appropriate persons for revoking access to any department IT assets.

When an Institute employee transfers to another department within the University system, the supervisor will:

1. Contact the local/regional IT representative or OIT HelpDesk to assist the employee with moving departmental and Institute data from the employee's assigned storage areas to a departmental storage area with the appropriate controls in place for least privilege access. (see UTIA IT01xx – *Information Technology Access Control Plan*).
2. Contact the appropriate persons for revoking access to any department and Institute IT assets.

Personnel Sanctions

Institute employees are expected to comply with this plan and all Institute IT policies, plans, and procedures. Failure to comply is addressed in UT Policy HR0525 – *Disciplinary Action*.

References:

UTIA Glossary of Information Technology Terms
UT Policy IT0130 – *Personnel Security Policy*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*
UTIA IT01xx – *Information Technology Access Control Plan*
UTIA IT0304P – *Network Registration Procedures*
UT Policy HR0525 – *Disciplinary Action*
UT System Human Resources Pre-Employment Background Checks
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 IT0130 – *Personnel Security Plan for Information Technology* 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		9/18/2017
Sandra D. Lindsey	Chief Information Security Officer, UTIA		9/14/2017