University of Tennessee Institute of Agriculture: UTIA IT0130 – Personnel Security Standard	
Version: 5.0	Effective Date: September 18, 2017

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

Scope:
This standard and its procedures apply to all Institute employees, which includes administration, faculty, staff, contractors, and student employees, as well as any persons outside the Institute with a legitimate and approved business need to access Institute IT assets or data.

Standard and Procedures
The standard and procedures are required for sustaining a formal, documented program to ensure that individuals who are granted access to systems and data, particularly systems and data classified as moderate, high, or business critical, are properly vetted so the information security objectives are maintained.

The standard and procedures are also required to ensure terminations or other employment changes are done in a timely and appropriate manner to ensure access to the Institute's IT assets and data is removed as soon as possible.

Position Risk Designation
The Institute's Office of Human Resources works with the University's Office of Human Resources to assign some form of risk designation to all organizational positions and establish screening criteria for individuals filling those positions. The risk designation will be an identifying factor based on roles and responsibilities for a given position. In addition, the Institute HR and UT HR offices review regularly and update those designations as necessary.

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/.

University of Tennessee Institute of Agriculture: UTIA IT0130 – Personnel Security Standard	
Version: 5.0	Effective Date: September 18, 2017

The appropriate Dean, Director, or Department Head is responsible for ensuring that affiliates, those 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 UTIA-owned 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.
3. Give listing of all Institute-owned data and where the data is being stored. Please remember that data is the property of the Institute, although you may have been responsible for that data. The only exception to this is a data owner who is explicitly written into a grant and/or research project.

Immediately upon termination of employment, the supervisor or their designated appointee will:

1. Ensure that any employee who will not be actively working goes through the official termination process, per UT Policy HR0160 – Termination of Employment.
   - See that all employees, including seasonal employees, are officially terminated.
   - Keep in mind that when not terminated properly, employees retain access to everything they had as an employee.
2. Contact the OIT HelpDesk to have a trouble ticket created and forwarded to the appropriate person(s) for having the IT assets reformatted and the operating system reinstalled after moving the data to the appropriate designated storage location.
   - Contact CVM Computer Support instead of the OIT HelpDesk if UTCVM faculty and staff.

Immediately upon termination of employment, the CISO will:

1. Remove any Institute-owned IT assets used by the employee from the University's network registration (NetReg) database. If the IT asset should not be removed from

the network, i.e., a server or asset that may be running certain processes, ownership will be temporarily reassigned.
2. Remove all personally-owned IT assets from the NetReg database.
3. Remove the employee from all Active Directory security and email groups in the UTIA organizational unit.
4. Contact the appropriate persons for revoking credentials associated with the terminated employee.

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 or the designated appointee will:

1. Contact the OIT HelpDesk or CVM Computer Support for creation of a trouble ticket for assisting 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 Standard).
2. Contact the appropriate persons for revoking access to any department IT assets.

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

1. Remove any Institute-owned IT assets used by the employee from the University's network registration (NetReg) database. If the IT asset should not be removed from the network, i.e., a server or asset that may be running certain processes, ownership will be temporarily reassigned.
2. Remove the employee from all Active Directory security and email groups for that department or unit.

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

1. Contact the OIT HelpDesk or CVM Computer Support for creation of a trouble ticket for assisting 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 Standard).

2. Contact the appropriate persons for revoking access to any department and Institute IT assets.

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

1. Remove any Institute-owned IT assets used by the employee from the University's network registration (NetReg) database. If the IT asset should not be removed from the network, i.e., a server or asset that may be running certain processes, ownership will be temporarily reassigned.
2. Remove all personally-owned IT assets from the NetReg database.
3. Remove the employee from all Active Directory security and email groups in the UTIA organizational unit.

Third-Party Personnel Security

All affiliates and third-party providers will comply with all UTIA IT Security Standards and Procedures. By signing the access agreement, the person is acknowledging that they have read and will comply with the Institute's AUP, as well as comply with all UTIA Standards and Procedures.

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. The CISO 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 Sanctions

All Institute employees are expected to comply with this standard and all other Institute IT standards and procedures. Failure to comply is addressed in UT Policy HR0525 – Disciplinary Action.

References:

UTIA Glossary of Information Technology Terms
UTIA IT0110 – Acceptable Use of Information Technology Resources Security Standard (AUP)
UTIA IT01xx – Information Technology Access Control Standard
UTIA IT0304P – Network Registration Procedures

University of Tennessee Institute of Agriculture: UTIA IT0130 – Personnel Security Standard	
Version: 5.0	Effective Date: September 18, 2017

UT Policy HR0160 – Termination of Employment
UT Policy HR0525 – Disciplinary Action
UT System Human Resources Pre-Employment Background Checks

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