UTIA IT0133 – Security Planning for Systems Policy

Effective: April 17, 2018
Last Reviewed: January 14, 2021 **Last Updated:** February 03, 2020

Objective:
This policy establishes how the University of Tennessee Institute of Agriculture (Institute) implements security planning by providing the minimum requirements for plan creation, implementation, and maintenance.

Scope:
This policy applies to information technology (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 assets classified as moderate, high, or business critical.

Policy:
The Institute develops and adheres to a formal, documented program to ensure that Security Policies provide an overview of security requirements and put in place the appropriate controls to address those requirements for Institute-owned IT assets classified as moderate, high, or business critical. All Institute Security Policies and Procedures are consistent with the requirements in Institute IT security policies and procedures; University policies; industry standards; and state, local, and federal laws. The appropriate controls for Security Planning Policies and Procedures are as follows:

<u>System Security Plan</u>
The Information System Owner:

- Submits a security plan for the IT asset that:
  1. Is consistent with the Institute's and UT Knoxville's (UTK) enterprise architecture;
  2. Explicitly defines the authorization boundary for the IT asset;
  3. Describes the operational context of the IT asset in terms of tasks and business processes;
  4. Provides the security classification of the IT asset including supporting rationale;
  5. Describes the operational environment for the IT asset, as well as the relationships with or connections to other IT assets;
  6. Provides an overview of the security requirements for each IT asset;
  7. Identifies any relevant overlaps, if applicable;
  8. Describes the security controls in place or planned for meeting the security requirements including a rationale for those decisions; and
  9. Is reviewed and approved by the Department Head or Director, Dean of the unit, the Institute's Chief Information Officer (CIO); and the Institute's Chief Information Security Officer (CISO) prior to plan implementation.

- Distributes copies of the security plan and communicates any subsequent changes to the Department Head or Director, and the appropriate Dean, the Institute's CIO, and the Institute's CISO;
- Reviews the security plan for the IT asset at least annually;
- Updates the plan to address changes to the IT asset or environment of operation, or problems identified during plan implementation or security control assessments; and
- Protects the security plan from unauthorized disclosure and modification.

Rules of Behavior

The Institute's CISO:

- Establishes rules of behavior and makes those rules available to anyone requiring access to the IT asset stated in the security plan;
  - These rules describe the user's responsibilities, and
  - These rules detail the expected behavior with regard to the IT asset, its usage, and its data;
- Receives a signed copy of the rules from each individual requiring access, acknowledging he/she has read, understands, and agrees to abide by the rules of behavior, prior to authorizing access to the IT asset;
- Reviews the rules of behavior at least annually, and updates as necessary; and
- Requires any individual who has previously signed a copy of the rules of behavior to read and sign any revised copy of the rules.

Central Management

The Institute centrally manages the implementation of all security controls and the related processes for Institute-owned IT assets. This central management includes planning, implementing, assessing, authorizing, and monitoring of such security controls and processes. Any user of Institute-owned IT assets is expected to follow all Institute security policies and procedures defining security controls. Any user of IT assets on the UTK network is expected to follow all UTK security policies and procedures with regards to network security.

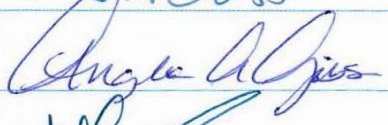
References:

UTIA Glossary of Information Technology Terms
UTIA IT0110 - Acceptable Use of Information Technology Resources Security Policy (AUP)
UT Policy IT0133 – Security Planning
UTIA IT0128 - Contingency Planning Policy
NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems

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

Approval of Policy

We approve UTIA IT0133 – Security Planning for Systems as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA		3/16/2020
Angela A. Gibson	Chief Information Officer, UTIA		3/20/2020
Sandra D. Lindsey	Chief Information Security Officer, UTIA		03/20/2020