UTIA IT0121 – INFORMATION TECHNOLOGY SECURITY PLAN

Effective: June 10, 2013
Last Reviewed: February 08, 2019 **Last Updated:** March 18, 2019

Objective:
The purpose of the Information Technology Security Plan (ITSP) is to describe the University of Tennessee Institute of Agriculture's (the Institute) strategy to protect users, data, and information systems; outline information security responsibilities; define the Authorization Boundary; and document current and planned security controls.

The Institute ITSP is a requirement of the UT Policy IT0121 – *Information Security Plan Creation, Implementation, and Maintenance*, which requires each campus and institute to create, approve, maintain, and implement an ITSP based on the National Institute of Standards and Technology (NIST) Risk Management Framework.

Scope:
This plan 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.

For the purposes of this ITSP, the Institute will be comprised of the following:

- Information Systems and Computing Equipment legally owned by the Institute.
- Information Systems and Computing Equipment administratively managed by the Institute.
- Information Systems and Computing Equipment connected (wired or wirelessly) to the University's networks.
- Information Systems and Computing Equipment connected to third party networks. Third party networks include those directly contracted for use by the Institute and those in use under special arrangements with the Institute.
- Institute employee's personally-owned equipment that use the University's networks and information.
- Information Systems and Computing Equipment belonging to the statewide University of Tennessee System Administration (UTSA) are considered out of scope. Examples: IRIS and ANDI
- Information Systems and Computing Equipment belonging to the University of Tennessee Knoxville campus (UTK) are considered out of scope. Example: Banner

"Information systems" includes computers, laptops, tablets, mobile, and network devices. All other systems and devices will be considered "foreign networks" in the context of this document.

Plan:

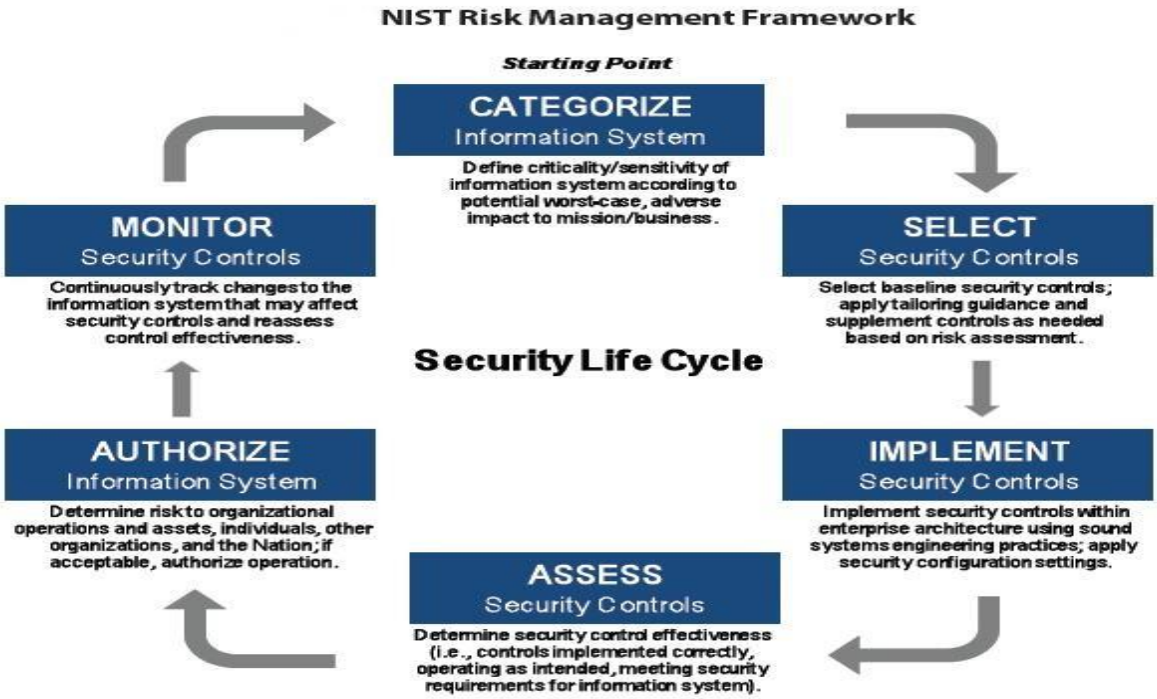
1. Goal

It is the goal of the Institute to implement a risk management framework that is consistent with relevant National Institute Standards and Technology (NIST) 800 Series Special Publications and with the Program Review for Information Security Management Assistance (PRISMA) methodology. The PRISMA methodology is a means of employing a standardized approach to reviewing and measuring the information security posture of an information security program. Achieving this goal will improve the information security posture, satisfy specific compliance requirements for the Institute, and provide individuals the information they need to protect Institute-owned IT assets.

- Visit the NIST Computer Security Division site for more information on NIST security plans.
- Review NIST SP 800-53 Rev. 4 – *Security and Privacy Controls for Federal Information Systems and Organizations* for detailed information on security controls.
- Review the PRISMA information for more details on the review and measuring process.

2. NIST Risk Management Framework

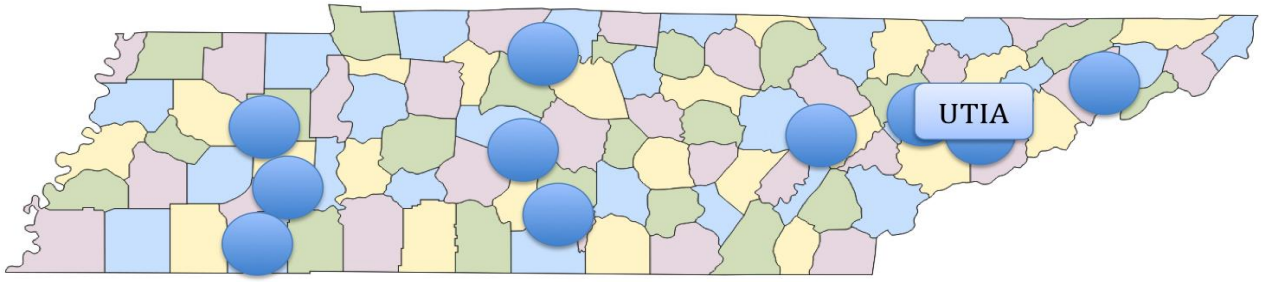
The NIST Risk Management Framework is defined below.



3. System Description

The University of Tennessee Institute of Agriculture is part of the University of Tennessee statewide system and the administrative staff is located on the Agricultural Campus of the University of Tennessee in Knoxville. The Institute has a wide-reaching presence with staff located in every county of the state. Each of these locations, including Extension regional and county offices, 4-H Centers, Research and Education Centers (REC), and the offices located on the Knoxville campus has university-supplied information technology (IT) resources available to them that must be protected.

Institute of Agriculture Locations



**UTIA Administration and Colleges are located in Knoxville; ten Research and Education Centers are positioned across the state; and UT Extension regional offices in Knoxville, Nashville and Jackson, and Extension county offices reside in each of Tennessee's 95 counties.*

UTIA is primarily comprised of four units: the Herbert College of Agriculture, College of Veterinary Medicine, Agricultural Research, and UT Extension.

- **The Herbert College of Agriculture** offers academic programs in a variety of natural and social science based disciplines that apply to the food, fiber, and natural resource systems. Faculty also supports students in various co-curricular activities from clubs and competition teams to professional and honor societies, as well as independent research and other creative endeavors.

- **The College of Veterinary Medicine (Vet Med)** is a veterinary college, which also serves pet owners, zoos, and the livestock industry, as well as protects public health, enhancing medical knowledge, and generating economic benefits to the state and nation.

- **Agricultural Research (AgResearch)** has basic and applied research programs on the Institute of Agriculture campus. AgResearch also has ten Research Centers across the state and, in partnership with Oak Ridge National Laboratory, makes the agricultural, forest, and ornamental industries more efficient, improves the quality of rural life, and conserves soil, water, air, and wildlife.

- **UT Extension (Extension)** is a statewide educational organization, funded by federal, state and local governments, that brings research-based information about agriculture, family and consumer sciences, resource development, and 4-H youth development to

the people of Tennessee. UT Extension is located on the Institute of Agriculture campus and has a presence in each of Tennessee's 95 counties.

4. Authorization Boundary

The Authorization Boundary identifies IT resources that fall into the Information Owner's scope of responsibility and defines the area where security controls will be applied.

- *The boundary explicitly excludes information systems, data, and information-handling processes outside of the established scope.*

Institute of Agriculture Authorization Boundary

External Systems and Entities, to include:
UTK provided services, such as:

- Email
- Office 365
- T-Storage
- Network security

UTSA provided services, such as:

- IRIS
- ANDI
- Cayuse

Within the Authorization Boundary reside major applications, Institute owned and hosted information systems, as well as faculty and staff computers.

Institute Major Applications

- System for University Planning Evaluation and Reporting (SUPER)
- CVM Student System
- CVM Hospital System

Institute Information Systems Central Facilities

- CVM Computer Center

Outside the authorization boundary are services and information systems not directly owned and managed by the Institute. Examples include UTK Office of Information Technology (OIT) services, such as email and departmental file shares.

Any application, system, department, or individual not included within the boundary is explicitly excluded from the Information Owner's scope of responsibility. The responsibility for securing such information and information systems lies with external entity's Information and Information System Owners.

5. Points of Contact and Responsibilities

Contact Information

The following is the point of contact for information regarding the UTIA ITSP:

Name: Sandra D. Lindsey
Title: Chief Information Security Officer
Email: sandy@tennessee.edu

Responsibilities

The following sections describe the roles and responsibilities of key participants involved in the risk management process. (Source: NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*)

Authorizing Official: The Authorizing Official is the senior official with the authority to accept risk for organizational operations (including mission, functions, image, or reputation.) This role authorizes the information system for operation based on the Information System Owner's certification that all controls are met or mitigated. This duty may be delegated to a designated representative.

Information System Owner: The Authorizing Official appoints this person in writing. The Information System Owner certifies that all information systems are operating within the required or compensatory control parameters. In areas where controls are not viable for business reasons the risk must be accepted in writing by the Authorizing Official. This role ensures that the system is deployed and operated in accordance with the ITSP.

Senior Information Security Officer: The Senior Information Security Officer is responsible for serving as the Chief Information Officer's primary liaison to the Institute's authorizing officials and information system owner(s). This role is responsible for the development, maintenance, and administrative approval of the ITSP.

The responsibility for these roles is assigned as follows:

- **Authorizing Official:** Dr. Tim Cross, Chancellor, UTIA
- **Information System Owner:** Angela Gibson, CIO, UTIA
- **Senior Information Security Officer:** Sandy Lindsey, CISO, UTIA

6. Information System Categorization

Information and systems will be classified according to Federal Processing Standard 199 (FIPS 199) and the guidance provided in University of Tennessee System Policy IT0115 and UTIA IT0115P – *Organizational Guidance for the Classification of Information and Systems*.

It is recommended that Institute and/or University information be classified as "Low" where appropriate or possible, and specific controls applied to cover compliance with laws, regulations, or standards.

a. Laws, Regulations, and Policies

- UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Policy (AUP)*
- Tennessee Code Annotated § 47-18-2107, 2010 S.B. 2793, *Release of personal consumer information*
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Payment Card Industry Data Security Standard (PCI DSS)

b. National Standards and Guidance

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199)
- NIST SP 800-53 Rev. 4 – *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-60 Volume I Revision I, *Guide for Mapping Types of Information and Information Systems to Security Categories (NIST 800-60 Volume I Revision 1)*
- NIST Special Publication 800-60 Volume I Revision II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories (NIST 800-60 Volume II Revision 1)*

c. University Policies

- **IT0121,** *Information Security Plan Creation, Implementation, and Maintenance*
- **IT0110,** *Acceptable Use of Information Technology Resources*
- **IT0115,** *Information and Computer System Classification*

7. Security Controls

The Institute will maintain a set of baseline controls that have been established in the UTIA IT Security Policies and Procedures using the NIST 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*. These controls are reviewed annually and updated as needed by the Institute's CISO. Any updates are reviewed by the UTIA Security Advisory Committee, Deans, Directors, Department Heads, and the Executive Committee, prior to approval by the Institute's CISO, CIO, and Chancellor.

The Institute shall work closely with UTK and UTSA to evaluate and implement Common Controls. The Institute shall develop Compensating Controls in cases where baseline controls are not adequate or do not fit the IT environment of the Institute.

Baseline Controls, based on NIST 800-53 Security Controls Catalog, minimum controls for any device or service protected by the University of Tennessee.

Common Controls are controls that are inheritable by one or more organizational information systems and will be inherited from many sources including, for example, the organization, organizational mission/business lines, sites, enclaves, environments of operations, or other information systems.

Compensating Controls are alternative security controls that provide protection for organizational information systems that do not meet the minimum controls defined in the baseline controls. These controls will be defined on an as needed basis. NIST-based baseline controls will normally take precedence over compensating controls.

8. Implementation

The implementation of the Institute ITSP shall occur in stages as defined by the NIST Risk Management Framework. The Institute shall self-certify its information and its information systems in order to complete the Categorization step.

References:

UTIA Glossary of Information Technology Terms
UT Policy IT0121 – *Information Security Plan Creation, Implementation, and Maintenance*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Policy (AUP)*
UTIA IT0115 – *Information and Computer System Classification Policy*
UTIA IT0115P – *Organizational Guidance for the Classification of Information and Systems*
UT Policy IT0115 – *Information and Computer System Classification*
NIST 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 UTIA IT0121 – *Information Technology Security Plan* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA	Tim Cross	4/15/2019
Angela A. Gibson	Chief Information Officer, UTIA	Angela Gibson	4/17/19
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/15/2019