THE UNIVERSITY of TENNESSEE

INSTITUTE of AGRICULTURE

Information Technology Security Plan (ITSP)

Effective Date: June 10, 2013

Date: 6/10/13

Larry Arrington
Chancellor, The University of Tennessee Institute of Agriculture

Date: 7-2-13

Caula Beyl
Dean of the College of The College of Agricultural Sciences and Natural Resources, The University of Tennessee Institute of Agriculture

Date: 6/10/13

Bill Brown
Dean of Agricultural Research, The University of Tennessee Institute of Agriculture

Date: 6/10/13

Tim Cross
Dean of Extension, The University of Tennessee Institute of Agriculture

Date: 6/10/13

Jim Thompson
Dean of the College of Veterinary Medicine, The University of Tennessee Institute of Agriculture

Date: 6/10/13

Robert Ridenour
Chief Information Officer, The University of Tennessee Institute of Agriculture

Table of Contents

1. Purpose

Every university employee is responsible and accountable for the security of university systems and information. Security compliance and accountability rests on the individual and failure to comply could result in fines and loss of state and/or federal funding. The responsibility and accountability is defined further in the University of Tennessee System Policy IT0110, Acceptable Use of Information Technology Resources Policy (AUP)**.**

The purpose of the IT security plan (ITSP) is to describe the University of Tennessee Institute of Agriculture's (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 completion of an Institute ITSP is a requirement of the University of Tennessee System Policy IT0121, 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.

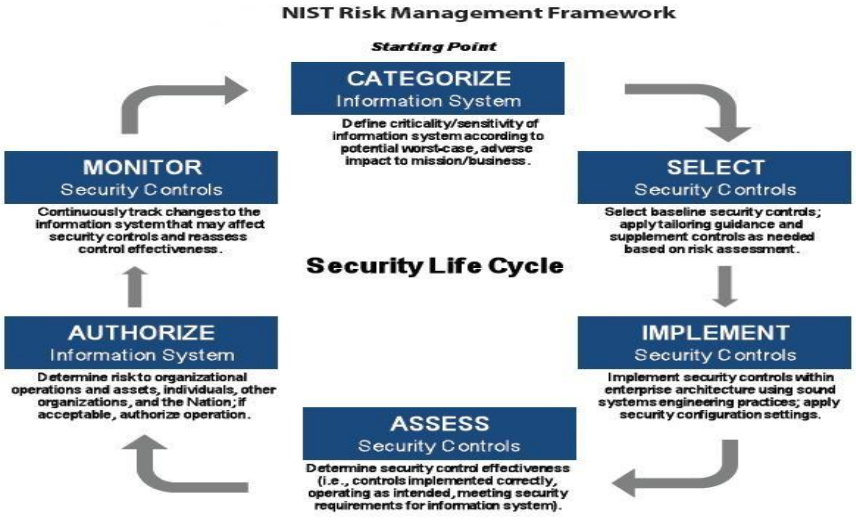
2. Goal

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 that 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 university assets.

- Visit the NIST Computer Security Division site for more information on NIST security plans.
- Take a look at NIST SP 800-53, Revision 4, *Recommended Security 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.

3. NIST Risk Management Framework

The NIST Risk Management Framework is defined below.



4. Scope

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 that is connected (wired or wirelessly) to the University's networks.
- Information Systems and Computing Equipment that is 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 networks and information.

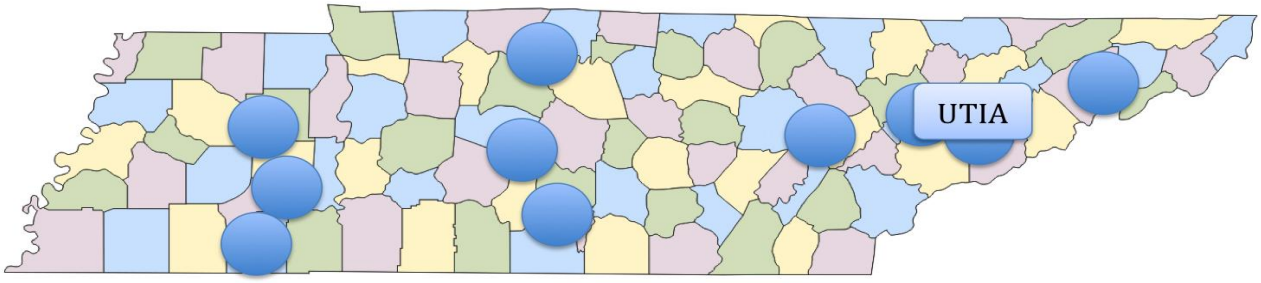
- Information Systems and Computing Equipment belonging to the statewide University of Tennessee System Administration (UTSA) are considered out of scope. Examples: TERA, IRIS, and ANDI
- Information Systems and Computing Equipment belonging to the University of Tennessee Knoxville campus (UTK) are considered 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.

5. 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, research and education centers (REC), and the offices locates 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 College of Agricultural Sciences and Natural Resources (CASNR), College of Veterinary Medicine (CVM), Agricultural Research, and UT Extension.

- **The College of Agricultural Sciences and Natural Resources (CASNR)** offers academic programs in a variety of natural and social science. Faculty also supports students in various co-curricular activities from clubs and competition teams to professional and honor societies, and independent research and other creative endeavors.

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

- **Agricultural Research (AgResearch)** with 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, and resource development to the people of Tennessee. UT Extension is located in each of Tennessee's 95 counties.

6. 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.

Examples Include:
UTK provided services such as:

- Email
- SharePoint hosting
- Network Security

UTSA Provided Services such as:

- IRIS
- ANDI
- TERA

Within the Authorization Boundary reside major applications, Institute owned and hosted information systems, and 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
- Plant Biotech Computer Center
- CVM Computer Center

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

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 information and information systems lies with external entity's Information and Information System Owners.

7. Points of Contact and Responsibilities

Contact Information

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

Name: Robert L. Ridenour, Jr.
Title: Chief Information Officer/Chief Security Officer
Email: ridenour@utk.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*)

Authorizing Official: 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 Owners 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 is responsible for the development, maintenance, and administrative approval of the ITSP. This role 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.

The responsibility for these roles is assigned as follows.
- Authorizing Official: **Dr. Larry R. Arrington**
- Information System Owner: **Robert L. Ridenour, Jr.**
- Senior Information Security Officer: **Robert L. Ridenour, Jr.**

8. 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 the associated Categorization Guide.

Guidance from the *University of Tennessee Guide for Mapping Types of Information and Information Systems to Security Categories* recommends that 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
- University of Tennessee System Policy IT0110, *Acceptable Use of Information Technology Resources*
- 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, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST 800-53).
- 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 1 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 1I Revision 1)*

c. University Policies
- **IT0121,** Information Security Plan Creation and Data Breach Notification Procedures
- **IT0110,** Acceptable Use of Information Technology Resources
- **IT0115,** Information and System Classification

9. Security Controls

The Institute will follow, as a minimum, the baseline controls defined by the University of Tennessee IT Security Community of Practice (CoP) Statewide Controls Baseline. The baseline controls document states:

"*In accordance with University of Tennessee policy IT0121, the IT Security program is based on the NIST Risk Management Framework. Within the Statewide IT Governance program, the IT Security Community of Practice has tailored the recommended controls from the NIST 800-53 Security*

Controls Catalog to create this minimum control baseline for any information systems or data protected by the University of Tennessee."

The Institute shall work closely with UTK and UTSA to evaluate and implement Common Controls. The Institute shall develop Compensation 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, 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. Example: changing UT NetID password.

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.

10. 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.