UTIA IT0121 – INFORMATION TECHNOLOGY SECURITY PROGRAM PLAN

Effective: June 10, 2013
Last Reviewed: August 01, 2021 **Last Updated:** August 13, 2021

Objective:
The purpose of the Information Technology Security Program 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 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.

Information Security Program Plan

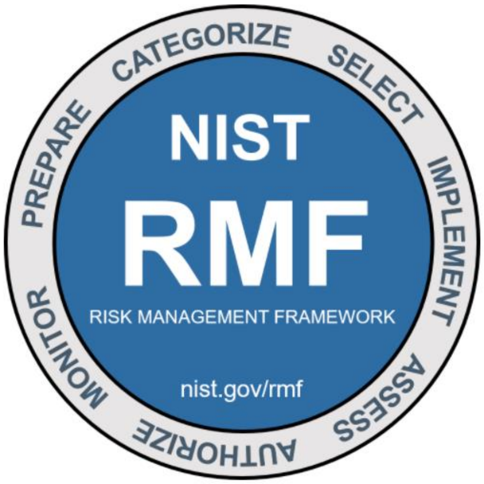
1. Goal

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. 5 – 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:



Prepare Step

Purpose: Carry out essential activities to help prepare all levels of the organization to manage its security and privacy risks using the RMF.

Outcomes:
- key risk management roles identified
- organizational risk management strategy established
- risk tolerance determined
- organization-wide risk assessment
- organization-wide strategy for continuous monitoring developed and implemented
- common controls identified

Categorize Step
Purpose: Inform organizational risk management processes and tasks by determining the adverse impact with respect to the loss of confidentiality, integrity, and availability of systems and the information processed, stored, and transmitted by those systems.

Outcomes:
- system characteristics documented
- security categorization of the system and information completed
- categorization decision reviewed/approved by authorizing official

Select Step
Purpose: Select, tailor, and document the controls necessary to protect the system and organization commensurate with risk.

Outcomes:
- control baselines selected and tailored
- controls designated as system-specific, hybrid, or common
- controls allocated to specific system components
- system-level continuous monitoring strategy developed
- security and privacy plans that reflect the control selection, designation, and allocation are reviewed and approved

Implement Step
Purpose: Implement the controls in the security and privacy plans for the system and organization.

Outcomes:
- controls specified in security and privacy plans implemented
- security and privacy plans updated to reflect controls as implemented

Assess Step
Purpose: Determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

Outcomes:

- assessor/assessment team selected
- security and privacy assessment plans developed
- assessment plans are reviewed and approved
- control assessments conducted in accordance with assessment plans
- security and privacy assessment reports developed
- remediation actions to address deficiencies in controls are taken
- security and privacy plans are updated to reflect control implementation changes based on assessments and remediation actions
- plan of action and milestones developed

Authorize Step
Purpose: Provide accountability by requiring a senior official to determine if the security and privacy risk based on the operation of a system or the use of common controls, is acceptable.

Outcomes:

- authorization package (executive summary, system security and privacy plan, assessment report(s), plan of action and milestones)
- risk determination rendered
- risk responses provided
- authorization for the system or common controls is approved or denied

Monitor Step
Purpose: Maintain ongoing situational awareness about the security and privacy posture of the system and organization to support risk management decisions.

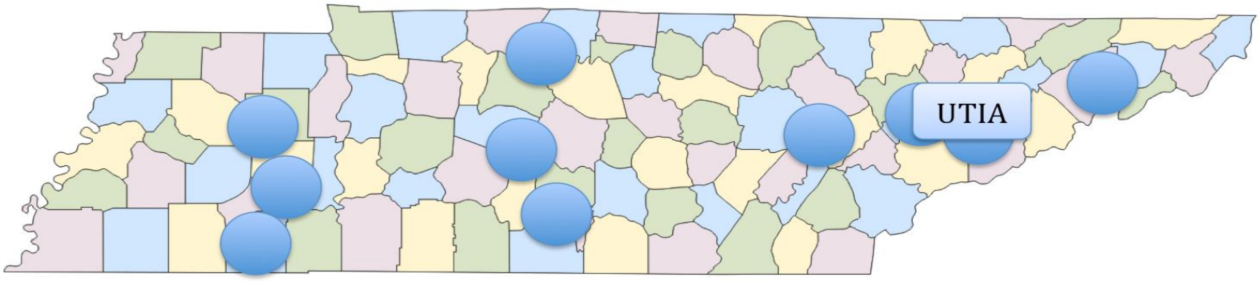
Outcomes:

- system and environment of operation monitored in accordance with continuous monitoring strategy
- ongoing assessments of control effectiveness conducted in accordance with continuous monitoring strategy
- output of continuous monitoring activities analyzed and responded to
- process in place to report security and privacy posture to management
- ongoing authorizations conducted using results of continuous monitoring activities

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 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 Institute-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.

Chief 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. Linda Martin, Interim Senior Vice President and Senior Vice Chancellor, UTIA
- **Information System Owner:** Angela Gibson, CIO, UTIA
- **Chief 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 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. 5 – 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)

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 Rev. 5 – 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.

Information Security Program Leadership Role

The Institute's Senior Vice President and Senior Vice Chancellor has appointed the Chief Information Security Officer (CISO) as the Institute's official with the mission and resources to coordinate, develop, implement, and maintain the Institute-wide information security program. The CISO is responsible for serving as the Chief Information Officer's (CIO) 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.

Information Security and Privacy Resources

The Institute's CIO will work with the Units to ensure there are resources available to implement the information security and privacy programs. The CIO will maintain an IT Security budget for departmental expenditures, while each Unit Budget Director will maintain budget information for the Units' IT Security Program expenditures.

IT Security Program expenditures are detailed in UTIA IT01xx – System and Services Acquisition Policy.

Plan of Action and Milestones Process

The Institute has implemented a process to ensure plans of action and milestones for the information security and privacy risk management programs and all Institute systems:

1. Are developed and maintained;
2. Document the remedial information security and privacy risk management actions to adequately respond to risk to Institute operations and assets, as well as the University; and
3. Are reported in accordance with the Institute's reporting requirements.

These processes are detailed in:
UTIA IT0131 – Security Assessment and Authorization Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy,
UTIA IT0124P1 – Information Technology Risk Assessment Procedures,
UTIA IT0124P2 – Vulnerability Assessment Procedures, and
UTIA IT0135 – System and Information Integrity Policy.

System Inventory

The Institute has developed an inventory of the Institute's systems using Manage Engine. This inventory is about what is on the system, rather than the actual system components.

The details of this inventory can be found in:
UTIA IT0125 – Information Technology Configuration Management Policy,
UTIA IT01xx – Information Technology Access Control Policy,

UTIA 0133 – Security Planning for Systems Policy, and
UTIA IT0135 – System and Information Integrity Policy.

Measures of Performance

The Institute has developed, and monitors and reports on the results of information security and privacy measures of performance. These measures of performance are outcome-based metrics used to measure the effectiveness and efficiency of the information security program.

The measures can be found in UTIA IT0131 – Security Assessment and Authorization Policy.

Enterprise Architecture

The Institute partners with UTK to maintain an enterprise architecture, due to the Institute using the UTK network. The details for this control can be found in:
UTIA IT0127 – Audit and Accountability Policy,
UTIA IT0127P – Audit and Accountability Procedures,
UTIA 0133 – Security Planning for Systems Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy, and
UTIA IT01xx – System and Services Acquisition Policy.

Critical Infrastructure Plan

The Institute addresses information security and privacy issues in the development, documentation, and updating of a critical infrastructure and business critical systems protection plan. This involves requirements detailed in:
UTIA IT0128 – Contingency Planning Policy,
UTIA IT0129 – Physical and Environmental Protection Policy,
UTIA IT0129P – Physical and Environmental Protection Procedures,
UTIA 0133 – Security Planning for Systems Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy, and
UTIA IT0135 – System and Information Integrity Policy.

Risk Management Strategy

As evidenced in this ITSP, the Institute has developed a comprehensive strategy to manage security and privacy risk to the Institute's operations and assets, individuals, the University, and any other affiliates. This strategy is consistently implemented across the Institute. In addition, the Institute reviews this strategy annually and updates, as necessary.

These policies make up the ITSP and this comprehensive strategy:
UTIA IT0110 – Acceptable Use of Information Technology Resource Security Policy (AUP),
UTIA IT01xx – Information Technology Access Control Policy,
UTIA IT0115 – Information and Computer System Classification Policy,
UTIA IT0115P – Organizational Guidance for Classification of Information and Systems,
UTIA IT0120 – Secure Network Infrastructure Policy,
UTIA IT0120P – Secure Network Infrastructure Procedures,
UTIA IT0122 – Information Security Incident Response Policy,

UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures,
UTIA IT0123 – Security Awareness, Training, and Education Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy,
UTIA IT0124P1 – Information Technology Risk Assessment Procedures,
UTIA IT0124P2 – Vulnerability Assessment Procedures,
UTIA IT0125 – Information Technology Configuration Management Policy,
UTIA IT0125P – Information Technology Change Control Procedures,
UTIA IT0127 – Audit and Accountability Policy,
UTIA IT0127P – Audit and Accountability Procedures,
UTIA IT0128 – Contingency Planning Policy,
UTIA IT0129 – Physical and Environmental Protection Policy,
UTIA IT0129P – Physical and Environmental Protection Procedures,
UTIA IT 0130 – Personnel Security Policy,
UTIA IT0131 – Security Assessment and Authorization Policy,
UTIA IT0132 – Identification and Authentication Policy,
UTIA IT0133 – Security Planning for Systems Policy,
UTIA IT0134 – System and Communications Protection Policy,
UTIA IT0135 – System and Information Integrity Policy
UTIA IT01xx – Media Protection Policy, and
UTIA IT01xx – System and Services Acquisition Policy.

Authorization Process

The Institute manages the security and privacy state of Institute-owned IT assets and the environments in which those assets operate using authorization processes. Employees are designated to fill specific role based on least privilege and need-to-know.

This control is detailed in UTIA IT0131 – Security Assessment and Authorization Policy and UTIA IT0133 – Security Planning for Systems Policy.

Mission and Business Process Definition

The Institute's mission and business processes are protected using a designated classification system to prevent loss of confidentiality, integrity, and availability. Controls are implemented based on classification of low, moderate, high, or business critical.

The details of these protections are found here:
UTIA IT0115 – Information and Computer System Classification Policy,
UTIA IT0115P – Organizational Guidance for Classification of Information and Systems,
UTIA IT0128 – Contingency Planning Policy,
UTIA IT0133 – Security Planning for Systems Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy,
UTIA IT0124P1 – Information Technology Risk Assessment Procedures,
UTIA IT0124P2 – Vulnerability Assessment Procedures, and
UTIA IT01xx – System and Services Acquisition Policy.

Security and Privacy Workforce

The Institute's CISO has developed and maintains a Security Awareness, Training, and Education Program to keep all those who access Institute-owned IT assets informed of IT security news, expectations, and current threats.

Details of this program can be found at UTIA IT0123 – Security Awareness, Training, and Education Policy.

Testing, Training, and Monitoring

The Institute has implemented a process for ensure that IT security testing, training, and monitoring is maintained and continues to be executed. The process is consistent with the Institute's risk management strategy.

Please see these policies for details at:
UTIA IT0123 – Security Awareness, Training, and Education Policy,
UTIA IT0131 – Security Assessment and Authorization Policy,
UTIA IT0128 – Contingency Planning Policy,
UTIA IT0122 – Information Security Incident Response Policy,
UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures, and
UTIA IT0135 – System and Information Integrity Policy.

Security and Privacy Groups and Associations

The Institute's CISO works with the other campus and institute CISOs to maintain a university-wide security community. In addition, the Institute's CISO works closely with the University's Audit and Compliance, Office of General Counsel, Office of Research and Engagement, Office of Sponsored Programs, Office of Human Resources, UT Police Department, InfraGard, FBI, Center for Internet Security, EDUCAUSE, and several other local, state, and national organizations to maintain knowledge of recommended security and privacy practices, techniques, and technologies, then incorporates those into the Institute's Security Awareness, Training, and Education Program. These connections are important to ensure our IT Security Program stays in line with all local, state, and federal laws, as well as industry standards and regulations.

Additional information is found in UTIA IT0123 – Security Awareness, Training, and Education Policy and UTIA IT0135 – System and Information Integrity Policy.

Threat Awareness Program

The Institute's CISO has implemented a threat awareness program that includes cross-Institute sharing of information with regards to threat intelligent.

Please see these policies and procedures for additional details:
UTIA IT0123 – Security Awareness, Training, and Education Policy,
UTIA IT0122 – Information Security Incident Response Policy, and
UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures.

Privacy Program Leadership Role

The Institute's Senior Vice President and Senior Vice Chancellor has appointed the CISO as the Institute's Data Protection Officer. As the Data Protection Officer, the Institute's CISO works with the University's Office of General Counsel and the other campus and institute Data Protection Officers to help regulate the privacy of users' personal data.

Accounting of Disclosures

The Institute's CISO is responsible for maintaining an accurate accounting of disclosure with regards to personally identifiable information. The records should include the date, nature, and purpose of each disclosure, as well as the appropriate information for the individual or organization to which the disclosure was made.

Additional information may be found in:
UTIA IT01xx – Information Technology Access Control Policy,
UTIA IT0127 – Audit and Accountability Policy, and
UTIA IT0127P – Audit and Accountability Procedures.

Data Governance Body

The Institute's CISO has established the Security Advisory Committee (SAC) which maintains the vision and plan for information technology (IT) security for the Institute. In addition, the SAC evaluates security issues that affect the Institute and develops responses that meet the Institute's operational needs and business objectives.

Additional objectives of the SAC can be found on the UTIAsecurity website under Committees.

Complaint Management

The Institute has multiple ways for individuals to register complaints, concerns, or questions about the Institute's security and privacy practices. These include going straight to the Institute's CISO, any other member of the Institute's leadership, or a member of the SAC.

Other information can be found in:
UTIA IT0122 – Information Security Incident Response Policy,
UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures, and
UTIA IT0135 – System and Information Integrity Policy.

Privacy Reporting

The Institute's CISO works with the Office of General Counsel for official privacy reporting. All privacy reporting from those with the Institute should follow UTIA IT0122 – Information Security Incident Response Policy and UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures.

Continuous Monitoring Strategy

The Institute partners with UTK for the use of LogRhythm. The Institute provides UTK's CISO with the information about our assets to be monitored and those assets are added to LogRhythm. Alerts are sent to the appropriate system administrators for analysis.

These policies are related to the continuous monitoring strategy:
UTIA IT0110 – Acceptable Use of Information Technology Resource Security Policy (AUP),
UTIA IT01xx – Information Technology Access Control Policy,
UTIA IT0115 – Information and Computer System Classification Policy,
UTIA IT0115P – Organizational Guidance for Classification of Information and Systems,
UTIA IT0120 – Secure Network Infrastructure Policy,
UTIA IT0120P – Secure Network Infrastructure Procedures,
UTIA IT0122 – Information Security Incident Response Policy,
UTIA IT0122P – Information Security Incident Response Plan and Reporting Procedures,
UTIA IT0123 – Security Awareness, Training, and Education Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy,
UTIA IT0124P1 – Information Technology Risk Assessment Procedures,
UTIA IT0124P2 – Vulnerability Assessment Procedures,
UTIA IT0125 – Information Technology Configuration Management Policy,
UTIA IT0125P – Information Technology Change Control Procedures,
UTIA IT0127 – Audit and Accountability Policy,
UTIA IT0127P – Audit and Accountability Procedures,
UTIA IT0129 – Physical and Environmental Protection Policy,
UTIA IT0129P – Physical and Environmental Protection Procedures,
UTIA IT0131 – Security Assessment and Authorization Policy,
UTIA IT0132 – Identification and Authentication Policy,
UTIA IT0133 – Security Planning for Systems Policy,
UTIA IT0134 – System and Communications Protection Policy,
UTIA IT0135 – System and Information Integrity Policy, and
UTIA IT01xx – System and Services Acquisition Policy.

Purposing

The Institute analyzes the use of IT-owned systems that provide business critical services or functions to ensure that those systems are being used in a way that is consistent with their intended purpose.

Please refer to the following policies:
UTIA IT0110 – Acceptable Use of Information Technology Resource Security Policy (AUP),
UTIA IT0131 – Security Assessment and Authorization Policy,
UTIA IT0133 – Security Planning for Systems Policy,
UTIA IT0124 – Information Technology Risk Assessment Policy,
UTIA IT0124P1 – Information Technology Risk Assessment Procedures, and
UTIA IT0124P2 – Vulnerability Assessment Procedures.

References:
UTIA Glossary of Information Technology Terms
UT Policy IT0121 – Information Security Plan Creation, Implementation, and Maintenance
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 Program Plan as described in this document.

Name	Title	Signature	Date
Tim L. Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA	DocuSigned by: Dr. Tim. L. Cross F81A83AFB474435...	8/25/2021 | 12:59:18 PDT
Angela A. Gibson	Chief Information Officer, UTIA	DocuSigned by: Angela A. Gibson 75409DE95BA8458...	8/26/2021 | 11:55:49 PDT
Sandra D. Lindsey	Chief Information Security Officer, UTIA	DocuSigned by: Sandra D Lindsey 213E082B08784A3...	8/27/2021 | 09:05:40 PDT