Objective:
Configuration management is essential for establishing and maintaining the integrity of the University of Tennessee Institute of Agriculture's (UTIA or Institute) information technology (IT) assets. This plan is designed to establish baseline configurations based on the overall needs of the Institute, as well as to define the need for asset management and change management, which are necessary parts of configuration management. The combination of these processes is important for initializing, changing, and monitoring the configuration of the Institute's IT assets.

Scope:
This plan applies to IT assets classified as moderate, high, or business critical that are owned, operated, or provided by the Institute and the network used by these IT assets, as well as all students, faculty, staff, and users who access, use, or handle the Institute's IT assets.

Plan:
Baseline Configuration
The Institute has developed a technical standard baseline for all IT assets. The Institute has a Technical Standards Committee that works with the Institute's Chief Information Security Officer (UTIA CISO) to review, maintain, and approve the technical baseline. The baseline standards,along with **a few** examples of each, are as follows:

1. IT Security Standards
   - Institute IT Security Plans and Procedures
   - Operating System Security Configurations
     - Local Security Policy
     - OS Firewall
2. University and Institute Business Processes
   - Accounts Payable
   - Accounts Receivable
   - IRIS
   - CVM Hospital Business Processes (those affected by technology)
   - 4-H Foundation
   - Extension QuickBooks
   - HR Processes
   - STRUT Soils Service

3. IT Support Processes
   - AgResearch Intranet
   - Bomgar Support, UTIA Instance
   - County Invoice System Support
   - CVM Computer Support
   - CVM Hospital Management System Support
   - Faculty Annual Reporting
   - Hardware Recommendations
   - LeadTRK Support
   - Master Producer
   - REC Data Portal
   - SHIELD Network Support
   - Software Support
     - Applications
     - Licensing
     - Use
   - SUPER Support
   - VetNet
   - Web Content Management System Support (WordPress)
   - Web Design/Maintenance
4. Infrastructure Architecture Standards
   - Virtual Server Platform
   - Network Infrastructure
   - Desktops/Laptops/Tablets
     - Hardware (any system approved under any University contract)
     - Operating System (vendor-supported OS; Windows must have AD support)
5. Data Architecture Standards
   - Defined by data processed, stored, and transmitted at the Institute
   - Format of the data is defined based on standards that promote consistency and sustainability.
6. Application Architecture Standards
   - Any licensed software package procured by university contract
   - Other department or unit reviewed and approved applications (not procured)

- Database Standards
    - MS SQL
    - MySQL (requires approval)
    - InterSystems Cache (CVM)
- Enterprise Applications
    - CVM Hospital System
    - CVM PACS Radiology
    - Master Gardner
    - Office of Sponsored Programs Grant Tracking (i.e., CAYUSE)
    - SPPC Soils Web App
    - SUPER
    - WordPress
- Web Technologies
    - HTML
    - CSS
    - JavaScript (jQuery, React, bootstrap, Angular)
    - PERL/CGI
    - ASP.net
    - C#
    - Python

All changes in technology shall be reviewed for compliance with the technical standards baseline. All new technologies must be reviewed by the Technical Standards Committee prior to implementation.

The Institute's change management process as defined in the UTIA IT0125P – Information Technology Change Control Procedures shall apply to all IT assets that are classified as moderate or high for the information they store, transit, or process (confidentiality and integrity) and all IT assets that are classified as business critical (availability). The UTIA IT0115 – Information and Computer System Classification Plan details the classification process for the Institute.

The Institute will focus on standard configurations for all IT assets, including desktops and laptops, as a part of this plan. Each Institute-owned IT assets will have a baseline configuration that will be used as the basis for future builds and changes. All Institute Windows-based desktops and laptops will be added to Active Directory (AD) and will have a desktop management client installed.

The baseline configuration(s) will be an agreed upon set of parameters based on system classification and user role-based access control. Systems will be configured to provide only the essential capabilities, using the principle of least functionality, which means non-essential services, functions, ports, and protocols must be restricted or disabled. Baseline configurations are reviewed at least annually and will be changed as necessary. A minimum of three previous configurations must be retained to support audit and rollback purposes.

Configuration Change Control
The UTIA IT0125P – Information Technology Change Control Procedures are in place to meet the Institute's changing IT needs and requirements. The change review process includes review of proposed changes to IT assets that are classified as moderate or high for the information they store, transit, or process (confidentiality and integrity) and all IT assets that are classified as business critical (availability) by the Institute's Change Advisory Team (CAT), which includes representation from each of the Institute's units.

Any user who needs a change for a moderate, high, or business critical IT asset that is not included in the baseline configuration must submit a Request for Change (RFC). Some requests may not have a long-term or direct impact on the Institute's business needs. These requests may have no need for a full review and vote, and may be designated as operational changes. The CAT will review the RFC and vote to approve or disapprove the change.

Security Impact Analysis
The Institute will analyze changes to its information systems to determine potential security impacts prior to change implementation. Security impact analyses may include the following:
-   Reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes may affect the controls.
-   Risk assessments to better understand the impact of the changes and to determine if addition controls are required.

Access Restrictions for Change
The Institute defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Only qualified and authorized individuals will be given access to information systems for the purposes of initiating changes, including any and all upgrades and modifications.

Configuration Settings

The UTIA CISO uses the Center for Internet Security's CIS Benchmarks for establishing, maintaining, and documenting configuration settings for operating systems and information technology products used within the information system using those benchmarks that reflect each classification type. The UTIA CISO works with the Endpoint Central Administrators to ensure these settings are implemented. The Desktop Central Administrators monitor and control changes to the configuration settings in accordance with the Institute's policies and procedures.

Least Functionality

The Institute requires that a properly configured information system will provide only those services and capabilities that are essential and will prohibit of restrict the use of specific functions, ports, protocols, and/or services.

Information System Component Inventory

The Institute's IT assets will be managed using known and approved management platforms like Desktop Central and the UT Knoxville Network Registration (NetReg) for systems; and ExtremeCloud IQ for access points and Global Management System for VPN appliances/firewalls. Desktop Central will be used to keep inventory records of where system hardware and software is located. The NetReg system will keep track of the primary user, as well as the classification. When an Institute-owned system is transferred from one user to another, the NetReg entry will be changed to show the correct owner and primary user. When a user is terminated, the NetReg entry will be deleted; the system will be wiped and reimaged; and the system will be registered in NetReg again when the asset is reassigned.

ExtremeCloud IQ for access points and Global Management System for VPN appliances/firewalls will be used to track the location, status, and configuration of Institute network hardware and software.

Configuration Management Plan

The Institute works with system administrators to develop, document, and implement configuration management plans for any information system classified as moderate or high. The configuration management plans are to include the following:
- Roles and responsibilities, as well as configuration management processes and procedures;

- Establishment of a process for identifying configuration items through the system development lifecycle and management of the configuration of a configuration item;
- Defining of the configuration items for the information system and places the configuration items under configuration management; and
- Protecting the configuration management plan from unauthorized disclosure and modification.

 Software Usage Restrictions
The Institute permits and uses only software and associated documentation in accordance with contract agreements and copyright laws. The Institute uses Desktop Central to determine who is using peer-to-peer file sharing technology.

User-Installed Software
The Institute will work with employees to determine if any software not on the approved list has a valid use. In the case of a researcher, the researcher should contact the UTIA CISO to inform ofthe need for that software. If anyone is wanting to purchase a new software not on the approved list and for the entire department, this will need to go through the Technical Standards Committee.

Roles and Responsibilities:
UTIA Chief Information Security Officer (UTIA CISO)
- Maintain UTIA IT0125 – Information Technology Configuration Management Plan
- Maintain UTIA IT0125P – Information Technology Change Control Procedures
- Provide guidance and assistance
- Chair the Technical Standards Committee
- Chair the Change Advisory Team

Technical Standards Committee
- Develop a baseline of technology standards, to include:
  a. Hardware,
  b. Software,
  c. Applications,
  d. Third party services, and
  e. Security tools;

- Maintain support documentation for the baseline standards;
- Evaluate new technologies using the TSM; and
- Determine necessary changes to the existing baseline.

Users/Information System Owners (Change Owners)
- Remain in compliance with the UTIA IT0125 – Information Technology Configuration Management Plan
- Document vendor-specific requirements
- Submit RFCs to the CAT, including all appropriate supporting documentation

CAT
- Review business-impacting RFCs for potential security impact
- Meet with Change Owners
- Document all change decisions
- Inform Desktop Central Administrators of approved changes

References:
UTIA Glossary of Information Technology Terms
UTIA IT0125P – Information Technology Change Control Procedures
UT Policy IT0125 – Configuration Management
UTIA IT0115 – Information and Computer System Classification Plan
UTIA IT0115P – Organizational Guidance for the Classification of Information and Systems
UTIA IT0302 – Information Technology Formal Exception Plan
UTIA IT0302F – Information Technology Policy Exception Request Form
NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

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

Approval of Plan

We approve UTIA IT0125 – Information Technology Configuration Management Plan as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA	*DocuSigned by:* Dr. Tim. L. Cross — E81AB3AEB474435	4/5/2021 | 11:25:21 PDT
Angela A. Gibson	Chief Information Officer, UTIA	*DocuSigned by:* Angela A. Gibson — 754C3DE85B46458	4/5/2021 | 11:30:22 PDT
Sandra D. Lindsey	Chief Information Security Officer, UTIA	*DocuSigned by:* Sandra D Lindsey — 213E082B08784A3	4/6/2021 | 04:01:23 PDT