UTIA IT0125 – Information Technology Configuration Management Policy

Effective: July 07, 2017
Last Reviewed: March 29, 2019 **Last Updated:** January 09, 2018

Objective:
Configuration management is essential for establishing and maintaining the integrity of the University of Tennessee Institute of Agriculture's (the Institute) information technology (IT) assets. This policy 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 policy 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.

Policy:
Baseline Configuration
The Institute shall develop a technical standards baseline for all IT assets. The Institute has a Technical Advisory Committee that will develop, review, and maintain the technical baseline. Items in the baseline include, but are not limited to:

- Server hardware and software
- Personal computer hardware and software
- Data architecture standards
- Network hardware and software
- IT support processes
- University and Institute business processes
- Application architecture standards

All changes in technology shall be reviewed for compliance with the technical standards baseline. All new technologies must be reviewed by the Technical Advisory 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 Policy* 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 policy. 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.

Asset Management

The Institute's IT assets will be managed using known and approved management platforms like SCCM and the UT Knoxville Network Registration (NetReg) system for systems and Aerohive Hive Manager for switches and access points and Global Management System for VPN appliances. SCCM 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.

Hive Manager for switched and access points and Global Management System for VPN appliances will be used to track the location, status, and configuration of Institute network hardware and software.

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 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.

Roles and Responsibilities:

Chief Information Security Officer (CISO)

- Maintain UTIA IT0125 – *Information Technology Configuration Management Policy*
- Maintain UTIA IT0125P – *Information Technology Change Control Procedures*
- Provide guidance and assistance

Users/System Administrators (Change Owners)

- Remain in compliance with the UTIA IT0125 – *Information Technology Configuration Management Policy*
- 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 SCCM Administrator of approved changes

References:

UTIA Glossary of Information Security Terms
UTIA IT0125P – *Information Technology Change Control Procedures*
UTIA Request for Change Form
UT Policy IT0125 – *Configuration Management*
UTIA IT0115 – *Information and Computer System Classification Policy*
UTIA IT0115P – *Organizational Guidance for the Classification of Information and Systems*
UTIA IT0302 – *Information Technology Formal Exception Policy*
NIST Special Publication 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 Policy

We approve UTIA IT0125 – *Information Technology Change Management Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		2/21/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		2/22/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		02/19/2018