

UTIA IT0125P – INFORMATION TECHNOLOGY CHANGE CONTROL PROCEDURES

Effective: July 07, 2017

Last Reviewed: October 15, 2018

Last Updated: November 07, 2018

Objective:

Change control activities are focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. This is important in establishing and maintaining secure information system configurations, baseline configurations, and supporting the management of security risks for the Institute's IT assets, including, but not limited to, desktops, laptops, servers, and networking equipment.

These change control procedures are created to accommodate the changing needs and requirements of the University of Tennessee Institute of Agriculture (the Institute), increasing visibility and communication of changes throughout the Institute. These procedures define the change management process and structure within the Institute. The inclusion of business partners in the testing and approval processes will also help the Institute work towards its goals of more comprehensive governance over IT functions, increased awareness of business process, and enhanced communications.

Scope:

These procedures 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) at the Institute.

Procedures:

The change control process includes the following:

- Establishing the Institute's Change Advisory Team (CAT);
- Submitting a Request for Change (RFC) for each change request;
- Entering all RFCs into a change management system for tracking and approval;
- Attaching all testing and approval documentation to the RFC and keeping for audit purposes; and
- Complying with the approved change management program.

The purpose of the CAT is to:

- Review the RFC, as submitted by the change owner.
- Review all documentation for completeness, evaluate the change request dates for conflicts with other scheduled Institute events or changes, and review the requests for compliance with the new change control procedures.
- Meet with change owner to discuss risks, as well as all testing and implementation plans.
- Approve/reject all changes to the Institute's Information Technology (IT) production environment based on established technical standards.
- Document configuration change decisions.
- Insure that all affected parties are aware of the change and its potential impact(s).
- Insure that the stability and reliability of IT production systems is maintained.
- Validate that only authorized changes go into production.
- Retain records of change.

The CAT meets as needed. The voting membership of the CAT is comprised of a Chair, which will be a rotating appointment among the five representatives below. These representatives are assigned by the Deans from each of the following units:

- AgResearch
- College of Veterinary Medicine
- Extension
- Herbert College of Agriculture
- Departments

Voting membership of the CAT will be reviewed every two years and membership may change at that time, if necessary. The Institute's Chief Information Security Officer (CISO) is responsible for maintaining the membership and naming the CAT Chair.

The CAT Chair has authority for the following:

- Decisions regarding what work is necessary to be submitted to the change process.
- Questions regarding procedure decisions, or CAT documentation interpretation.
- Serves as the mediator for instances of conflicts and/or critical issues.

When a requested change affects a specific business unit, representation from that unit will be requested to appear at the CAT session with the change owner. This is often necessary to validate the impact. Others are invited to attend the CAT meeting as necessary or where there may be other interested parties.

RFCs will be scheduled for review at a specified CAT meeting where all five CAT members are in attendance. If an appointed CAT member cannot be in attendance, a replacement may be selected for that meeting. The CAT member must choose someone from the unit for which he/she has been assigned, and that replacement must be knowledgeable about the RFC(s) being discussed at that meeting. While the CISO is not a voting member, she may fill in for the

CAT Chair and vote if the Chair is unavailable. For an RFC to be approved, it must be a majority decision. An RFC will be rejected if there is reason to postpone the vote until any necessary edits to the RFC have been made. Only emergency RFCs may be voted on electronically.

References:

[UTIA Glossary of Information Security Terms](#)

[UTIA IT0125 – Information Technology Configuration Management Plan](#)

[UTIA Request for Change Form](#)

[UT Policy IT0125 – Configuration Management](#)

[UTIA IT0115 – Information and Computer System Classification Plan](#)

[UTIA IT0302 – Information Technology Formal Exception Plan](#)

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

Approval of Procedures

We approve UTIA IT0125P – *Information Technology Change Control Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		11/19/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		11/19/18
Brent Lamons	Director of Advising and Student Success, Herbert College of Agriculture		11/19/18
Mark Young	IT Coordinator, AgResearch		11/19/18
Emily Tipton	IT Coordinator, Extension		11/19/18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		11/19/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		11/19/18
JC Rains	Extension Agent and County Director, Bledsoe County		11/19/18