UTIA IT0128 – CONTINGENCY PLANNING POLICY

Effective: April 17, 2018
Last Reviewed: March 28, 2019 **Last Updated:** February 22, 2018

Objective:
This policy details the contingency planning program for the University of Tennessee Institute of Agriculture (the Institute). Contingency planning is necessary for managing the risk of any Institute IT asset failure or service disruption.

Scope:
This policy applies to all Institute-owned IT assets classified as business critical, including IT network infrastructure that is not considered a part of the University of Tennessee Knoxville (UTK) network, as well as all IT assets connected to the Institute's network infrastructure. In addition, this policy applies to the Institute's administration, staff, contractors, student employees, and visitors. Individuals with permanent physical access, such as employees, contractors, and others, with permanent physical access authorization credentials are not considered visitors. The appropriate UTK security policies and procedures apply to all Institute IT assets housed in the UTK-managed data centers and network closets and should be referenced in the contingency plan.

Policy:
The Institute's Contingency Planning Program must consist of each of the following controls:

- Contingency Plan
- Contingency Training
- Contingency Plan Testing
- Alternate Storage Site
- Alternate Processing Site
- Information System Backups
- Information System Recovery and Reconstitution

<u>Contingency Plan</u>
The owner/primary user of the IT asset classified as business critical:

- Develops a contingency plan for the IT asset that includes:
  1. Essential missions and business functions, along with the associated contingency requirements;
  2. Recovery objectives, restoration priorities, and metrics;
  3. Contingency roles, responsibilities, and assigned individuals with internal and external contact information;

4. Maintenance of essential missions and business functions regardless of any IT asset disruption, compromise, or failure;
5. Full information system restoration without deterioration of any security safeguards originally planned and implemented; and
6. Review and approval by the Department Head or Director, Dean of the unit, and the Institute's Chief Information Security Officer (CISO).

- Distributes copies of the contingency plan to all individuals with roles and responsibilities defined in the contingency plan;
- Coordinates contingency planning activities with incident handling activities (see UTIA IT0122 – *Information Security Incident Response Policy* and *UTIA IT0122P – Information Security Incident Response and Reporting Procedures*);
- Reviews the contingency plan at least annually;
- Updates the contingency plan to address any changes to the Institute, the IT asset, or the environment of operation, as well as any problems encountered during contingency plan implementation or testing;
- Communicates any changes to the contingency plan to the Department Head or Directory, Dean of the unit, and the Institute's CISO; and
- Protects the contingency plan from unauthorized disclosure and modification.

In addition to the above details, the contingency plan must also address the system restoration and alternative processes for when systems are compromised. The contingency plan must reflect the degree of restoration necessary for Institute-owned IT asset(s), since not all IT assets must be fully recovered to achieve the desired level of continuity of operations. The contingency plan must also document the alternate storage site and alternate processing site information.

Contingency Training

The Institute will direct staff with a contingency role or responsibility to appropriate contingency training consistent with said role or responsibility. Such staff must be trained within 30 days of assuming a contingency role or responsibility and must be trained at least annually or when required by IT asset changes.

Contingency Plan Testing

The owner/primary user of the IT asset classified as business critical:

- Tests the contingency plan for the IT asset at least annually to determine the effectiveness of the contingency plan and the readiness to execute the plan;
- Reviews the contingency plan test results; and
- Initiates corrective actions, if necessary.

Methods for testing a contingency plan to determine the effectiveness of the plan include walk-through and tabletop exercises, checklists, simulations, and comprehensive exercises. These methods also identify potential weaknesses in the contingency plan.

Alternate Storage Site

The owner/primary user of the IT asset classified as business critical:

- Establishes an appropriate alternate storage site;
- Ensures that the alternate storage site provides IT security protections equivalent to that of the primary site; and
- Establishes a plan or agreement for alternate telecommunications services at the alternate storage site.

Alternate storage sites are geographically distinct from primary storage sites. The alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Alternate storage sites must also meet the requirements in UTIA IT 01xx – *Information Technology Access Control Policy*, UTIA IT0129 – *Physical and Environmental Protection Policy*, and UTIA IT0129P – *Physical and Environmental Protections Procedures*.

Alternate Processing Site

The owner/primary user of the IT asset classified as business critical:

- Establishes an appropriate alternate processing site;
- Ensures that equipment and supplies required to transfer and resume operations are available and can be delivered if necessary;
- Ensures that the alternate processing site provides IT security protections equivalent to that of the primary site; and
- Establishes a plan or agreement for alternate telecommunications services at the alternate processing site.

Alternate processing sites are geographically distinct from primary processing sites. The alternate processing site maintains duplicate copies of information and data in the event that the primary processing site is not available. Alternate processing sites must also meet the requirements in UTIA IT 01xx – *Information Technology Access Control Policy*, UTIA IT0129 – *Physical and Environmental Protection Policy*, and UTIA IT0129P – *Physical and Environmental Protections Procedures*.

Information System Backups

The owner/primary user of the IT asset classified as business critical:

- Conducts regular backups of user-level information contained in the IT asset;
- Conducts regular backups of system-level information (i.e., operating system, application software, and licenses) contained in the IT asset;
- Conducts regular backups of IT asset documentation, including security-related documentation; and
- Protects the confidentiality, integrity, and availability of backup information at storage locations.

Protecting the integrity of the IT asset backup can be done by using digital signatures and cryptographic hashes. Backups should be stored at the chosen alternate storage location.

Information System Recovery and Reconstitution

Information system recovery and reconstitution is also called disaster recovery. The owner/primary user of the IT asset classified as business critical will execute the contingency plan activities to restore the IT asset. Once recovery has taken place, reconstitution begins for returning the IT asset to a fully operation state. Reconstitution includes deactivating any interim IT asset capabilities that may have been necessary for recovery operations, as well as assessments of the fully restored IT asset capabilities, establishment of continuous monitoring activities, and activities to prepare the IT asset against future disruptions, compromises, or failures.

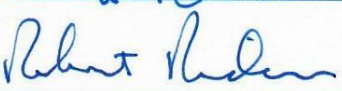
References:

UTIA Glossary of Information Technology Terms
UT Policy IT0128 – *Contingency Planning*
UTIA IT0115 – *Information and Computer System Classification*
UTIA IT0122 – *Information Security Incident Response Policy*
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
UTIA IT 01xx – *Information Technology Access Control Policy*
UTIA IT0129 – *Physical and Environmental Protection Policy*
UTIA IT0129P – *Physical and Environmental Protection Procedures*
NIST SP 800-34 – *Contingency Planning Guide for Federal Information Systems*

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

Approval of Policy

We approve UTIA IT0128 – *Contingency Planning Policy* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		4/17/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		4/17/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		4/16/2018