UTIA IT0129P – Physical and Environmental Protection Procedures

Effective: April 25, 2018
Last Reviewed: February 08, 2018 **Last Updated:** February 08, 2018

Objective:
This document describes the details for implementing UTIA IT0129 – *Physical and Environmental Protection Plan*.

Scope:
These procedures apply to all Institute-owned IT assets, 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, these procedures apply 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 plans and procedures apply to all Institute network infrastructure housed in the UTK-managed data centers and network closets.

Procedures:
Physical Access Authorizations
Access to any Institute-owned IT asset classified as business critical must be limited to authorized employees only. The Institute's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or their designee will be responsible for:

- Developing, approving, and maintaining a list of individuals with authorized access to the facility where the IT assets reside;
- Ensuring the issue of authorization credentials (i.e., UT ID card/badge) for non-public facility access;
- Reviewing the access list detailing authorized facility access by individuals;
- Removing individuals from the facility access list immediately when access is no longer required or when the individual terminates.

Physical Access Control
For business critical IT assets the Institute's CIO, CISO, or their designee will be responsible for:

- Enforcing physical access authorizations at entry/exit points where these IT assets are housed by
    1. Verifying individual access authorizations prior to granting access;
    2. Controlling traffic into and out of the facility by requiring swipe access or physical sign-in;

    3. Restricting access to delivery areas by keeping separate from IT assets and media libraries.
- Maintaining physical access audit logs by
    1. Ensuring access to electronic logs for swipe access;
    2. Keeping paper logs for physical check-in where swipe access is not possible.
- Ensuring doors to the facility are locked during non-business hours or when offices are left unattended, or that security cameras are installed and monitored where appropriate.
- Escorting visitors and monitoring the activity.
- Securing keys, codes, or other physical access devices (e.g., locks, card readers, etc.).
- Maintaining inventory of keys, codes, or other physical devices at least annually, or when changes are made.
- Ensuring that keys, codes, or other physical devices are changed when keys are lost, codes are compromised, or individuals no longer require access or are terminated.

Access Control for Transmission Medium

Network equipment and wiring must be protected by storing in locked rooms or cabinets so that only authorized individuals may access. Doors must be locked and clearly marked showing restricted areas. Also, refer to UTIA IT0120P – *Secure Network Infrastructure Procedures*.

Access Control for Output Devices

Institute-owned output devices, such as monitors, multifunction printers, scanners, fax machines, audio devices, projectors, etc., must be protected from unauthorized access by

- Placing devices in secured areas or in offices that are locked when unattended;
- Securely configuring devices, allowing only authorized users to access; and
- Configuring printers, scanners, and fax machines to securely erase any data that is sent through these devices.

Power Equipment and Cabling

Power equipment and cabling to any Institute-owned IT assets must be protected from damage and destruction. Protecting the power equipment and cabling can be achieved by

- Using cord and cable covers, where possible, to protect from pedestrians or equipment when cords and cables are lying out in high-traffic areas; and
- Visibly inspecting power equipment and cabling on a regular basis and replace any cords or cables that show signs of damage.

Emergency Power

Institute-owned IT assets classified as business critical must be protected by uninterruptible power supply (UPS). The UPS will provide short-term emergency power in the event of a primary power source loss. The UPS will also protect these IT assets during power spikes, reduction in input voltage, and other power problems. IT assets storing data classified as

moderate or high should also be protected by the use of UPS or other standby power generator if possible.

Alternate Work Site

The Institute's CISO makes the cell phone number public so that he/she may be reached in the event of a security incident, security concerns, or other emergency situations. Please refer to UTIA IT0128 – *Contingency Planning*.

Location of Information System Components

Institute-owned IT assets are to be placed within the appropriate facilities in a way to minimize potential damage from physical and environmental hazards.

- IT assets will be placed on a desk or other location off the floor in areas prone to flooding.
- IT assets will be placed out of the path of electrical interference and other forms of incoming electromagnetic radiation.
- IT assets will not be placed near any unattended door as to protect them from vandalism, theft, or unauthorized access.

Asset Monitoring and Tracking

Accurate records of all Institute-owned IT assets should be kept by the appropriate person within the unit, department, center, or county.

- All Institute-owned IT assets must be monitored and tracked through annual inventory. Please refer to UT Policy FI0605 – *Equipment*.
- These records must be immediately updated when any change occurs.
- Any Institute-owned IT asset that is classified as business critical may not be moved from its authorized location. Should there be a legitimate need to move these types of assets, the Institute's CIO, CISO, or their designee must be notified in writing prior to moving.

References:

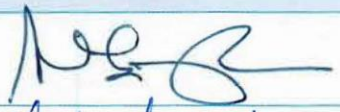
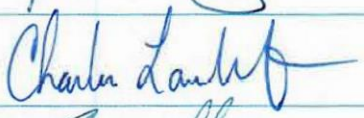
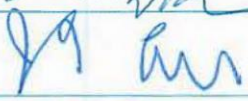
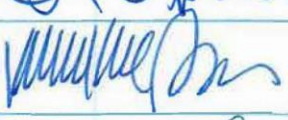
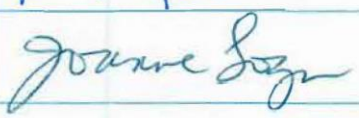
UTIA Glossary of Information Technology Terms
UTIA IT0129 – *Physical and Environmental Protection Plan*
UT Policy IT0129 – *Physical and Environmental Protection*
UTIA IT0120 – *Secure Network Infrastructure Plan*
UTIA IT0120P – *Secure Network Infrastructure Procedures*
UTIA IT0128 – *Contingency Planning*
UT Policy FI0605 – *Equipment*
NIST SP 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST SP 800-12 – An *Introduction to Computer Security: The NIST Handbook*
NIST Special Publication 800-100 – *Information Security Handbook: A Guide for Managers*

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

Approval of Procedures

We approve UTIA IT0129P – *Physical and Environmental Protection Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/25/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		4/20/18
Brent Lamons	Director of Advising, Herbert College of Agriculture		4/20/18
Joel Lown	Coordinator, AgResearch		4/20/18
Emily Tipton	IT Coordinator, Extension		4/23/18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		4/20/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		4/20/18