UTIA IT0129 – PHYSICAL AND ENVIRONMENTAL PROTECTION PLAN

Effective: April 17, 2018
Last Reviewed: March 02, 2018 **Last Updated:** March 02, 2018

Objective:
This plan is to provide best practices regarding the physical and environmental protection of facilities where the University of Tennessee Institute of Agriculture (the Institute) maintains Institute-owned IT assets.

Scope:
This plan applies 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, this plan 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 plans and procedures apply to all Institute network infrastructure housed in the UTK-managed data centers and network closets.

Plan:
The Institute will implement the following controls for Physical and Environmental Protection. Please note that while this plan applies to all Institute-owned IT assets, some controls apply directly to those IT assets classified as business critical. Please see UTIA IT0129P – *Physical and Environmental Protection Procedures* for details of each control.

Physical Access Authorizations
Physical access authorizations apply to employees and visitors accessing Institute-owned IT assets classified as business critical. The Institute's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or their designee will be responsible for ensuring that only those individuals who need access are authorized with the appropriate credentials.

Physical Access Control
Physical access control applies to Institute employees and visitors accessing any Institute-owned IT assets classified as business critical, moderate, and high. The Institute's CIO, CISO, or their designee will be responsible for ensuring physical access is in place and maintained at facilities where these business critical IT assets reside.

Access Control for Transmission Medium

Network equipment and wiring are protected by storing in locked rooms or cabinets, with access limited to authorized individuals. Please refer to UTIA IT0120 – *Secure Network Infrastructure Plan* and UTIA IT0120P – *Secure Network Infrastructure Procedures*.

Access Control for Output Devices

Output devices may include, but are not limited to multifunction printers, scanners, and fax machines. Access to these output devices is limited by placing them in areas, such as secured areas or offices that are locked when unattended, where unauthorized use is prevented. In addition, these devices must be configured so only authorized users may access them and so all data is securely erased after transmission.

Power Equipment and Cabling

Power equipment and power cabling for Institute-owned IT assets must be protected from damage and destruction, and should be regularly inspected, as such. Power equipment and cabling includes, but is not limited to generators, power cabling outside of buildings, internal cabling, and uninterruptable power supplies (UPS).

Emergency Power

Power to Institute-owned business critical IT assets must be protected by UPS to ensure continuity of services during power outages, as well as to protect from potential damage due to power irregularities. If any IT asset stores data classified as moderate or high, that asset should also be protected using a UPS or standby power generator, if possible.

Alternate Work Site

The Institute will define alternate work sites as a part of contingency operations. The Institute's CISO will assess, as feasible, the effectiveness of security controls at these alternate sites and provide a means for employees at these sites to communicate with the CISO in the event of security incidents or issues. Please refer to UTIA IT0128 – *Contingency Planning*.

Location of Information System Components

The Institute will place its IT assets within the appropriate facility to minimize potential damage from physical and environmental hazards, such as fire, floods, tornados, earthquakes, vandalism, electrical interference, acts of terrorism, etc. The Institute will also protect these IT assets by placing them where the physical entry points give minimal chance of unauthorized access.

Asset Monitoring and Tracking

The Institute must keep accurate records of its IT assets, which is done through annual inventory. Should any Institute-owned IT asset need to be moved, reassigned, or retired, records must be updated at once. Business critical IT assets must remain in authorized locations.

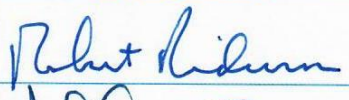
References:

UTIA Glossary of Information Technology Terms
UTIA IT0129P – *Physical and Environmental Protection Procedures*
UT Policy IT0129 – *Physical and Environmental Protection*
UTIA IT0120 – *Secure Network Infrastructure Plan*
UTIA IT0120P – *Secure Network Infrastructure Procedures*
UTIA IT0128 – *Contingency Planning*
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 Plan

We approve UTIA IT0129 – *Physical and Environmental Protection Plan* 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		04/16/2018