UTIA IT0120P – Secure Network Infrastructure Procedures

Effective: February 16, 2018
Last Reviewed: April 01, 2019 **Last Updated:** January 22, 2018

Objective:
Network management activities focuses on establishing and maintaining the integrity of Institute's networks and systems, through control of the processes for initializing, changing, monitoring, and maintaining the configurations of network. This is important in establishing and maintaining secure network configurations and supporting the management of security risks for the networks operated and maintained by the University of Tennessee Institute of Agriculture (the Institute).

These procedures seek to protect the network infrastructure in order to meet the Institute's mission of teaching, learning, research, and community service. These procedures detail how the Institute provides a reliable and secure network infrastructure through network wiring, as well as maintenance and monitoring of the network infrastructure.

Scope:
These procedures applies to the Institute's IT network infrastructure that is owned and operated by the Institute only. All Institute employees using UTK network infrastructure must follow the appropriate UTK security policies and procedures.

Procedures:
Network Management

- Network equipment is housed in dedicated storage enclosures. One key to each enclosure is provided to on-site personnel and one key is provided to the designee.
- All network equipment owned and operated by the Institute shall be maintained by trained Institute IT personnel only.
- Access to all network equipment and management systems are password protected and access is granted to trained Institute IT personnel only. The passwords are changed on a yearly basis and distributed securely to the IT personnel.
- Access to all network equipment and management systems shall be competed using secure protocols only.
- Change access to the management interface for the VPN appliances shall be restricted to the primary IT personnel responsible for management of the VPN appliances. Read access shall be granted based on a need-to-know basis only.
- Change access to the management interface for the access points and switches shall be restricted to the primary IT personnel responsible for management of these devices. Read access shall be granted based on a need-to-know basis only.

- All network infrastructure components shall be maintained at a reasonable operational and secure level. All critical network equipment shall be replaced on a five-year cycle.

Network Wiring

- All construction and renovation projects involving network infrastructure must be validated in writing by the Institute's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or their designee.
- The wired infrastructure shall be installed by Institute approved IT personnel or Institute approved designees. The requirements include, but are not limited to:
    1. Two network drops per office.
    2. Four network drops per conference rooms.
    3. One network drop for audio-visual instance.
    4. Minimum of 2-inch conduit for room entry for all connections.
    5. A designated IT communications location that is managed and maintained by the Institute.
- Plans for accessing the data communications enclosures and infrastructure must be documented and signed by the Director and the IT designee.
    1. If access is not made available to personnel 24x7x365, or during office hours where building access is not attainable due to the property being owned by an entity other than the Institute, there must be clear directives stating how access will be attained.
    2. Access to buildings not owned by the Institute will be negotiated with the property owner and those directives will be included in this documentation.
    3. The County or Center Director will keep the copy of the signed access plans, and must email an electronic copy to the IT designee, the Extension/AgResearch IT coordinator, and the Institute's CISO.

Monitoring and Maintenance

- Monitoring of the current status of the Institute network hardware shall be accomplished using the network monitoring tool developed by the ITS department.
- All network infrastructure devices shall have logging capabilities enabled to record all access attempts, both successful and unsuccessful. The Institute's trained Institute IT personnel shall review the logs of network activity at least monthly and upon the determination of a security event.
- All network infrastructure devices shall be maintained at the most recent stable code levels that provide the highest required level of security. The code levels shall not be more than two versions behind the most recent industry approved version.
- There shall be a pre-determined maintenance window established for all network infrastructure devices that provides sufficient time on a regular basis to maintain the hardware and software updates.

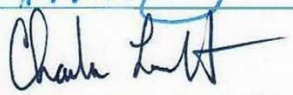
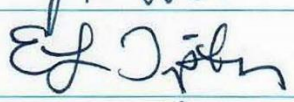
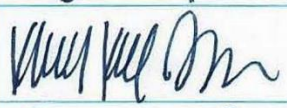
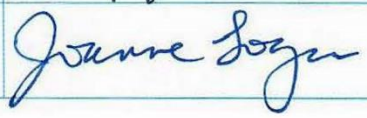
References:

UTIA Glossary of Information Security Terms
UTIA IT0120 – *Secure Network Infrastructure Policy*
UT Policy IT0120 – *Secure Network Infrastructure*
UTIA IT0125 – *Information Technology Configuration Management Policy*
UTIA IT0125P – *Information Technology Change Control Procedures*
UTIA Request for Change Form
UTIA IT0302 – *Information Technology Formal Exception Policy*
UTIA IT0302F – *Information Technology Policy Exception Request Form*

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

Approval of Procedures

We approve UTIA IT0120P – *Secure Network Infrastructure Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		02/16/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		2/16/18
Brent Lamons	Director of Advising, Herbert College of Agriculture		2/16/18
Joel Lown	Coordinator, AgResearch		2/15/18
Emily Tipton	IT Coordinator, Extension		2-16-18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		2/16/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		2/22/18