

UTIA IT0120 – SECURE NETWORK INFRASTRUCTURE PLAN

Effective: September 18, 2017

Last Reviewed: January 22, 2018

Last Updated: January 22, 2018

Objective:

The University of Tennessee Institute of Agriculture (the Institute) must protect its network infrastructure in order to meet its mission of teaching, learning, research, and public service. This plan details how the Institute is providing a reliable and secure network infrastructure through network wiring, as well as maintenance and monitoring of the network infrastructure.

Scope:

This plan 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 plans and procedures.

Plan:

General

- The Institute deploys standards, procedures, and controls to address specific or unique requirements.
- The Institute has established a process to evaluate requests for non-standard solutions (see [UTIA IT0125 – Information Technology Configuration Management Plan](#), [UTIA IT0125P – Information Technology Change Control Procedures](#), [UTIA IT0302 – Information Technology Formal Exception Plan](#)).
- This plan applies to construction and renovation projects involving network infrastructure, and the Institute's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or their designee must be consulted for project-related network requirements.
- The Institute is developing a disaster recovery and emergency response plan covering its critical network infrastructure. They will include input from the information custodians and the Institute's Chief Business Officer.
- A stated from the AUP, users shall not:
 1. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) to the network without prior approval from the Campus IT organization.
 2. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth.
- Deviation from the policies outlined in this plan or the procedures found in the [UTIA IT0120P – Secure Network Infrastructure Procedures](#) must be documented.

1. Any finding of deviation must be recorded by the IT designee, who will send an email notification to the County Director, Regional Director, Center Director, and the Institute's CISO.
2. If the deviation cannot be remediated, a [UTIA IT0302F – Information Technology Plan Exception Request Form](#) must be submitted for review.

Network Wiring

- The connectivity infrastructure, wired and wireless, is the responsibility of the Institute and must only be installed and maintained by or under the direct supervision of the CIO, CISO, or designee, according to the established national standards.
- Access to network infrastructure, including switches, routers, and ISP equipment, must be limited to appropriate and approved personnel.
- The requirements and design of appropriate space for network equipment enclosures in new construction and renovations is the responsibility of the CIO, CISO, or designee.
- Data communications enclosures and infrastructure must be accessible to appropriate 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. Access to buildings not owned by the Institute will be negotiated with the property owner.

Monitoring and Maintenance

- Network infrastructure components must be maintained at a reasonable operational and security level.
- The Institute's information technology organization will monitor and maintain the availability and integrity of the network infrastructure. The management of the network system will be approved by the CIO, CISO, or designee.
- Critical network components must log significant events according to the approved [UTIA IT0120P – Secure Network Infrastructure Procedures](#).
- The Institute has adopted a sparing strategy that accounts for the critical network infrastructure by providing regionally-based spare equipment.
- The Institute has adopted a strategy that provides sufficient time on a regular basis to maintain the network infrastructure.
- Administrative access to network components must utilize secure access methods. In cases where insecure protocols must be used, documented compensating controls must be in place.
- All backups of network infrastructure devices must be secured in a locked storage facility.

References:

[UTIA Glossary of Information Technology Terms](#)

[UTIA IT0120P – Secure Network Infrastructure Procedures](#)

[UT Policy IT0120 – Secure Network Infrastructure](#)

[UTIA IT0110 – Acceptable Use of Information Technology Resources Security Plan \(AUP\)](#)

[UT Policy IT0110 – Acceptable Use of Information Technology Resources](#)

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

[UTIA IT0125P – Information Technology Change Control Procedures](#)




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

[UTIA IT0302F – Information Technology Plan Exception Request Form](#)

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

Approval of Plan

We approve the UTIA IT0120 – *Secure Network Infrastructure Plan* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		2/21/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		2/22/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		02/19/2018