

## UTIA IT0134 – SYSTEM AND COMMUNICATIONS PROTECTION PLAN

**Effective:** April 17, 2018

**Last Reviewed:** March 05, 2018

**Last Updated:** March 09, 2018

### **Objective:**

This plan establishes the system and communications protection policy in order to protect the confidentiality, integrity, and availability (CIA) of information technology (IT) assets owned by the University of Tennessee Institute of Agriculture (the Institute), as well as the data on those IT assets.

### **Scope:**

This plan applies to IT assets owned, operated, or provided by the Institute that are classified as moderate, high, and business critical, as well as all students, faculty, staff, and users who access, use, or handle those Institute-owned assets. All users of Institute-owned IT assets must also follow UT Knoxville’s (UTK) IT security plans and procedures where the UTK network and its parts and processes are involved.

### **Plan:**

The Institute-owned IT assets covered by this plan are protected by using the following security controls:

#### Denial of Service Protection

The Institute relies on UTK’s Office of Information Technology (OIT) to provide denial of service (DoS) protection, as OIT owns the network that the Institute is using in the Knoxville area. OIT uses a number of methods to protect the UTK network from DoS attacks, including the network firewall, routers, and load balancers. For those users on the Institute’s statewide network, the network will be protected from DoS attacks through the use of firewalls, routers, and cloud services protections.

The Institute’s Chief Information Security Officer (CISO) is responsible for maintaining [UTIA IT0122 – Information Security Incident Reporting and Response Plan](#) and [UTIA IT0122P – Information Security Incident Response and Reporting Procedures](#), which define how incidents, such as a DoS attack, will be handled and reported.

#### Boundary Protection

The Institute relies on OIT to provide boundary protection, as OIT owns the network that the Institute users are connecting to in the Knoxville area. OIT uses a number of methods to protect the UTK network’s internal and external boundaries. For those users connecting to the

Institute's statewide network, the internal and external network boundaries will also be protected.

Managed interfaces used by OIT and the Institute include routers, firewalls, network-based malicious code analysis and virtualization systems, and encrypted tunnels implemented within the security architecture.

#### Cryptographic Key Establishment and Management

The Institute relies on OIT to provide cryptographic key management, as OIT owns the network that the Institute users are connecting to in the Knoxville area. For those administrators managing the Institute's statewide network, the network will also be protected by the use of cryptographic key management.

Cryptographic keys are strings of bits used to transform plain text into cipher text or vice versa. Cryptographic key management deals with the generation, exchange, storage, use, destruction, and replacement of cryptographic keys. Cryptographic key management will be done in accordance with all Institute plans and procedures; University policies; applicable local, state, and federal laws; and other applicable directives, policies, regulations, standards, and requirements.

#### Collaborative Computing Devices

Collaborative computing devices, such as networked (interactive) whiteboards, cameras, and microphones, will be configured to prohibit remote activation, except where remote activation is explicitly allowed and provides explicit indication of use to users who are physically present at the devices. Explicit indication of use includes signals to users when collaborative computing devices are activated. These devices must be disabled or removed after each use, as not to allow subsequent compromises of the Institute's information, such as eavesdropping on conversations when the devices are not properly disabled or removed.

#### Secure Name/Address Resolution Service (Authoritative Source)

The Institute relies on OIT for name and address resolution as OIT owns the domain name system (DNS) servers that affect all users of Institute-owned IT assets.

#### Secure Name/Address Resolution Service (Recursive or Caching Resolver)

The Institute relies on OIT for name and address resolution as OIT owns the domain name system (DNS) servers that affect all users of Institute-owned IT assets.

#### Architecture and Provisioning for Name/Address Resolution Service

The Institute relies on OIT for name and address resolution as OIT owns the domain name system (DNS) servers that affect all users of Institute-owned IT assets.

**References:**

[UTIA Glossary of Information Technology Terms](#)

[UTIA Policy IT0134 – System and Communication Protection](#)




[UTIA IT0122 – Information Security Incident Reporting and Response Plan](#)

[UTIA IT0122P – Information Security Incident Response and Reporting Procedures](#)

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

## Approval of Plan

We approve UTIA IT0134 – *System and Communications 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		4/16/2018