THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0120-M - Secure Network Infrastructure Program	
Version: 4	Effective Date: 08/22/2024

Objectives:

To establish a formal, documented program for the creation and maintenance of secure network infrastructure.

Scope:

This program applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this program is based on those guidelines.

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a User accesses, uses, or handles University resources.

UT - Martin Policy: IT0120-M - Secure Network Infrastructure Program	
Version: 4	Effective Date: 08/22/2024

Program Details:

This program provides guidance on how Information Technology Services (ITS) provides secure and reliable network infrastructure to the University of Tennessee at Martin. This program covers all networks, devices, and services connected to the UTM network.

See *IT0110 - Acceptable Use of Information Technology Resources* for further restrictions and exceptions.

Roles and Responsibilities:

Chief Information Officer (CIO): Has overall accountability of this Secure Network Infrastructure Program as the Position of Authority.

Director of IT Security: Responsible for overseeing the implementation, monitoring, and maintenance of this program.

Construction and Renovation Projects:

The CIO or their designee must be consulted for project-related network requirements.

Disaster Recovery and Emergency Response:

See *IT0128-M – Contingency Planning* for additional information on disaster recovery.

See UTM's *Emergency Response Plan* for additional information on emergency response.

Network Wiring:

The connectivity infrastructure, both wired and wireless, shall only be installed and maintained by or under direct supervision of the CIO or their designee.

Access to communications infrastructure shall be limited to appropriate and approved personnel. Equipment should be housed in dedicated enclosures, where possible.

The requirements and design of appropriate space for data communication enclosures in new construction and renovations is the responsibility of the CIO or their designee.

Data communications infrastructure and enclosures shall be accessible to appropriate personnel 24x7x365.

UT - Martin Policy: IT0120-M - Secure Network Infrastructure Program	
Version: 4	Effective Date: 08/22/2024

Monitoring and Maintenance:

Network infrastructure components shall be maintained at a reasonable operational and security level. An equipment refresh cycle in accordance with industry standards related to end-of-life timeframes shall be implemented and followed.

The availability and integrity of the network infrastructure shall be monitored.

Critical network components shall log significant events.

Sufficient time shall be provided on a regular basis to maintain the communications infrastructure. See *IT0135-M - System and Information Integrity Program* for details.

Administrative access to network components shall utilize secure access methods.

All backups of network infrastructure devices shall be secured at the same level as the primary device.

Related Services

ITS shall establish and maintain control of the Internet Protocol (IP) network address space, including both dynamic and static addressing, and the Domain Name System (DNS).

Non-Standard Solutions

Requests for non-standard solutions shall be evaluated and approved by the Network Administrator, Director of Infrastructure, and the CIO.

References:

IT0120 - Secure Network Infrastructure

IT0110 - Acceptable Use of Information Technology Resources

IT0128-M - Contingency Planning (Non-public)

IT0135-M - System and Information Integrity Program

Emergency Response Plan