THE UNIVERSITY OF TENNESSEE
MARTIN

| UT - Martin Policy:<br>IT0134-M - System and Communication Protection Program | |
|---|---|
| Version: 3 | Effective Date: 12/13/2022 |

## Objectives:

To establish a formal, documented system and communication protection program for critical information systems (SC-1) to ensure compliance with requirements established by the University.

## 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. This program is based on guidelines in *NIST Special Publication 800-53 Revision 5.1, Security and Privacy Controls for Information Systems and Organizations*.

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:<br>IT0134-M - System and Communication Protection Program | |
|---|---|
| Version: 3 | Effective Date: 12/13/2022 |

## Program Details:

This program is designed to help maintain the confidentiality, availability, and integrity of business-critical information assets and data (in transit and at rest).

This program applies to IT systems that are designated business-critical by the Position of Authority. The following table shows information on business-critical systems:

| Business-Critical Systems | | | |
|---|---|---|---|
| System | Subsystem | Owner/Administrator | Contact |
| Banner | Servers | Application Development/Administration and Operations | Systems Analyst/Administrator |
| Banner | Database | Application Development/Administration and Operations | Senior Database Administrator |
| Banner | Applications | Application Development/Administration and Operations | Systems Analyst/Administrator |

NOTE: This table will be updated as systems are determined to be business-critical and the configuration change control processes are developed.

## Roles and Responsibilities:

Chief Information Officer: Has overall accountability of this System and Communication Protection Program as the Position of Authority.

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

| UT - Martin Policy:<br>IT0134-M - System and Communication Protection Program | |
|---|---|
| Version: 3 | Effective Date: 12/13/2022 |

### Network Protection:

UTM utilizes a Next-Generation Firewall (NGFW) for boundary protection (SC-7) and Denial-of-Service (DoS) attack protection (SC-5).

### Cryptographic Key Management (SC-12):

UTM establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with University policy.

### Collaborative Computing Devices and Applications (SC-15):

Business-critical systems prohibit the remote activation of collaborative computing devices and applications without an explicit indication to local users.

### Secure Name/Address Resolution Service (Authoritative Source) (SC-20):

Name/address resolution service provides appropriate additional data origin and integrity artifacts (e.g. digital signatures, etc.) along with the authoritative data it returns in response to queries.

### Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21):

Name/address resolution services of critical information systems perform data origin authentication and data integrity verification on resolutions received from authoritative sources.

### Architecture and Provisioning for Name/Address Resolution Service (SC-22):

UTM has deployed fault-tolerant systems for name/address resolution services.

### Annual Review:

This program must be reviewed annually (SC-1).

| UT - Martin Policy:<br>IT0134-M - System and Communication Protection Program | |
|---|---|
| Version: 3 | Effective Date: 12/13/2022 |

References:

*IT0134 - System and Communication Protection*

*NIST SP 800-53 Revision 5.1, Security and Privacy Controls for Information Systems and Organizations*

Definitions:

**Boundary Protection -** Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).

**Cryptographic Key -** A string of bits used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.

**Denial of Service (DoS) -** Actions that prevent a system from functioning in accordance with its intended purpose. A system may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

**Next-Generation Firewall (NGFW) -** Combines the functions of a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS).