THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0121-M - Information Security Plan	
Version: 5	Effective Date: 10/12/2022

Objective:

To describe how the security program is executed and the controls implemented or planned to support it.

Scope:

This plan 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. Specifically, this plan is based on the Risk Management Framework detailed in *NIST SP 800-37 Revision 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

UTM must develop or adopt and adhere to a plan that demonstrates compliance with related policies and standards. This plan 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: IT0121-M - Information Security Plan	
Version: 5	Effective Date: 10/12/2022

Plan Details:

The UTM Information Security Plan defines:

- Identification and assignment of related security responsibilities including who is responsible for accepting risk
- A description of the baseline controls in place or planned for meeting the security requirements
- Interconnecting systems and related Interconnection Security Agreements (ISAs)
- A listing of critical applications and systems

Roles and Responsibilities:

The following sections identifies the roles and responsibilities of key participants involved in the University's information security program.

Authorizing Official: The senior official with the authority to accept risk for organizational operations (including mission, functions, image, or reputation). This role authorizes the information system for operation based on the Information System Owners certification that all controls are met or mitigated. This duty may be delegated to a designated representative. Assigned to the Chancellor.

Information System Owner: The Authorizing Official appoints this person in writing. The information system owner, most often the campus/institute's Chief Information Officer (CIO), is responsible for the development, maintenance, and administrative approval of the security plan. This role certifies that the information systems are operating with all required or compensatory controls. In areas where controls are not viable for business reasons, the Authorizing Official must accept the risks in writing. This role ensures that the system is deployed and operated in accordance with that plan. Assigned to the CIO.

Senior Information Security Officer: This role approves compensatory measures for required security control. The organizational official administers the information system security program at each location and is responsible for carrying out the Information Security Officer's security program. Assigned to the Assistant CIO or Director of IT Infrastructure.

System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The System Owner has the authority to accept the level of risk for the system or sub-system operations. This role certifies that the Information System has the acceptable level of security controls or compensating controls are implemented, or that or a Plan of Action exists for mitigation of risks.

UT - Martin Policy: IT0121-M - Information Security Plan	
Version: 5	Effective Date: 10/12/2022

Information Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The Information Owner has the authority to accept the level risk to the confidentiality, integrity, and availability of the information.

Plan Review:

This information security plan should be reviewed annually and updated, as necessary.

System Description:

The University of Tennessee at Martin is the University of Tennessee System's campus in Northwest Tennessee. The University of Tennessee at Martin is comprised of one campus in Martin, TN and five centers in Jackson, Parsons, Ripley, Selmer, and Somerville. The university enrolls about 7,000 students at the Martin campus and at its various centers.

Critical Systems:

See Appendix C (*IT0121-M-C - Critical Applications and Systems)* for more information regarding critical applications and systems.

Controls:

See Appendix A *(IT0121-M-A - Mandatory and Discretionary Controls*) for the controls implemented or planned by UTM to satisfy the requirements of UT System IT policies.

Risk Management:

The University has adopted the NIST Risk Management Framework for risk management.

Incident Response:

UTM has developed and implemented a Security Incident Response Plan which outlines how the campus identifies, reports, and responds to Security Incidents.

More information can be found in *IT0122-M - Security Incident Response Plan*.

System Boundaries:

The UTM ITS system is made up of two major networks at the main campus plus the regional centers.

The regional centers connect to the main campus network via private metro Ethernet provided by Charter Communications.

The main campus networks are the Staff/Faculty and Residence Zones. The network is further divided into the general use network for all LAN traffic / non-confidential information assets and several protected network zones where information systems dealing with confidential information reside. A Palo Alto Networks Next Generation Firewall (NGFW) separates the general use and protected network zones to allow traffic between the two for officially requested ports or protocols. The NGFW also functions as UT Martin's Intrusion Prevention System and URL web filter in all zones.

IT Resources:

The UTM Office of Information Technology Services (ITS) is the central IT service provider for the UTM main campus and centers. IT resources fall into two primary categories:

- ITS managed resources: Includes managed workstations, such as lab computers; ITS data center - servers and applications hosted in a physically secure, environmentally controlled environment; central IT services - messaging, central authentication services (Active Directory), DNS, DHCP, and student information systems; network infrastructure - provides connectivity on campus to other UT locations and to areas off campus; and various servers managed and hosted by ITS.
- Personally or departmentally managed resources: Workstations and servers managed by individuals (faculty, staff, or students) or departments. Although these resources may leverage ITS managed systems such as the network infrastructure or ITS data center, the department or individual is ultimately responsible for the operation and security of these resources.

Out-of-Scope Systems:

UTM hosts and connects to systems and networks that are outside UTM's scope of responsibility from an IT risk perspective. Where applicable, interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, nondisclosure agreements, etc. can be used for the interconnection.

Appendix B (*IT0121-M-B - System Information Exchanges)* lists interconnections established outside the scope of this information security plan (e.g., internet service providers, cloud services, etc.).

Areas Requiring Supplemental Plans:

Some subsystems or networks may require additional controls depending on information classification, industry regulation, system requirements, and/or legal requirements. The most common of these include:

- The Payment Card Industry Data Security Standard (PCI-DSS)
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- The Health Insurance Portability and Accountability Act (HIPAA)

UT - Martin Policy: IT0121-M - Information Security Plan	
Version: 5	Effective Date: 10/12/2022

System and Information Classification:

System owners must determine the criticality and sensitivity of information being processed, stored, or transmitted by information systems to apply the appropriate information security controls. This is done through information security categorization to determine the appropriate controls that must be applied.

UT Policy *IT0115 - Information and Computer System Classification* requires campuses to categorize information systems based on FIPS 199 to determine the impact to security objectives.

Information System and Information Classification			
	Potential Impact		
Information Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Adverse Effects Definitions:

A limited adverse effect is characterized by:

- minor degradation in mission capability and effectiveness of primary functions
- minor damage to University assets
- minor financial loss

A serious adverse effect is characterized by:

- significant degradation in mission capability and effectiveness of primary functions
- significant damage to University assets
- significant financial loss

A severe or catastrophic adverse effect is characterized by:

- severe degradation in or loss of mission capability and inability to perform primary functions
- major damage to University assets
- major financial loss

References:

NIST SP 800-37 Revision 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

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

IT0115 - Information and Computer System Classification

FIPS Publication 199 - Federal Information Processing Standards Publication - Standards for Security Categorization of Federal Information and Information Systems

IT0121 - Information Security Plan Creation, Implementation, and Maintenance

IT0121-M-A - Mandatory and Discretionary Controls

IT0121-M-B - System Information Exchanges

IT0121-M-C - Critical Applications and Systems

IT0122-M - Security Incident Response Plan