THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RM-001-Risk Management	
Version 4	**Effective Date: 09/23/2020**

Responsible Office: Office of Cybersecurity	Last Review: 01/11/2023 Next Review: 01/11/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish a process to manage risks to the University that result from threats to the confidentiality, integrity, and availability of UTHSC's data and information systems. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This Standard applies to all UTHSC data and systems; regardless of technology, that transmits, stores, utilizes, or manipulates said data. This standard is applicable to all UTHSC employees, and students, as well as to third-party agents/vendors authorized to access UTHSC data.

Definitions

Data owner - The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division

Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring

Risk Assessment - The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system

System owner - Person or organization having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system

System Security Plan (SSP) – formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Responsibilities

Chief Information Security Officer (CISO) is responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this standard.

Security Analyst is responsible for providing security guidance for protection of PII, ePHI, and other sensitive information to the UTHSC community. This role along with the CISO is responsible for the adherence of this policy.

System/Data Owner is responsible for performing the various steps related to identifying potential risks and threats and are required to ensure that identification of risks is properly categorized and documented in terms of their potential threat to their college, department, or area. The system and data owner(s) are then responsible to develop the risk mitigation plan and work towards complete mitigation of identified risks. All information regarding risks to the business systems will be the responsibility of the System Data Owner, or appointed delegate, to document, track and respond whenever appropriate.

Standard

1. All Information Systems must be assessed for risk that results from threats to the integrity, availability, and confidentiality of UTHSC data. Assessments should be completed using the guidelines set forth in RM-001.01-Risk Assessment Process prior to purchase of, or significant changes to, an Information System; and at least annually for systems that store, process or transmit Level 3 data per GP-002-Data & System Classification.
2. Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.
3. Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by the Chief Information Security

Officer. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.

4. Each Information System must have a system security plan, prepared using input from risk, security, and vulnerability assessments.
5. Exceptions to this Standard should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices

References

1. RM-001.01-Risk Assessment Process
2. GP-002-Data & System Classification
3. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices