THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RM-004 Third Party Risk Management	
Version 1	**Effective Date: 06/29/2023**

Responsible Office: Office of Cybersecurity	Last Review: 06/29/2023 Next Review: 06/29/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The Third-Party Risk Management (TPRM) program, governed by Information Technology Services is an initiative to reduce the risk to University Data and computing resources from Third-Parties, Service Providers, and Vendors. Information Security collaborates with the Technology Review Team, Contracts and Legal Teams, Procurement Office, Privacy Officers, and University Departments to protect Information Technology Resources and digital intellectual property at the University.

The purpose of this standard is to ensure that all vendors have appropriate controls to minimize risks that could adversely impact the Confidentiality, Availability, and/or Integrity of University Data. This standard is also designed to meet compliance requirements for data types 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 store, process, or transmit University data. This standard is applicable to all UTHSC employees, as well as to third-party agents/vendors authorized to access UTHSC data.

Definitions

Availability - The principle of ensuring timely and reliable access to and use of Information based upon the concept of Least Privilege.
Confidentiality - The principle of preserving authorized restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary information.

Data - Data is element(s) of information in the form of facts, such as numbers, words, names, or descriptions of things from which "understandable information" can be derived.

Employee - University staff and faculty, including nonexempt, exempt, and overseas staff and collegiate faculty.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Technology Resource(s) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by UTHSC directly or by a third party under a contract with UTHSC which requires the use of such equipment. The term includes computers, mobile devices, software, firmware, services (including support services), and UTHSC's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Information System - Inter-related components of Information Resources working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Integrity - Ensuring records and the Information contained therein are accurate and Authentic by guarding against improper modification or destruction.

Least Privilege - The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

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.

Third-Party - Third-Party is an external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, with or without a contractual relationship to the university.

Responsibilities

ITS Executive Leadership is accountable for executing and implementing third-party relationship risk management strategies and policies across the organization. Executive Leadership is also responsible for ensuring that organizational structures, management, and staffing (level and expertise) are in place to properly manage third-party risk and comply with all legal and regulatory requirements. Furthermore, Senior Leadership is accountable for the following:

- Developing and implementing the University's third-party risk management process.
- Confirming that the University has an appropriate system of internal controls and regularly tests the controls to manage risks associated with third-party relationships.
- Confirming that the University's compliance management process is appropriate to the nature, size, complexity, and scope of its third-party business arrangements.
- Confirming that appropriate due diligence and ongoing monitoring are conducted on third parties.
- Presenting results to Executive Leadership when making recommendations to use third parties that involve critical activities.
- Escalating significant issues to Executive Leadership
- Confirming that critical third parties comply with University policies and reporting requirements.
- Providing that third parties test and implement agreed-upon remediation when issues arise.
- Terminating business arrangements with third parties that do not meet expectations or no longer align with University strategic goals, objectives, or risk appetite.

The ITS Technology Review Team is responsible for performing security and architectural reviews in alignment with the Third-Party Risk Management Processes. Reviews include:

- Identifying, measuring, monitoring, and controlling risks of third-party relationships.
- Involving multiple disciplines across the organization as appropriate during each phase of the third-party risk management lifecycle.
- Confirming appropriate staffing and expertise to perform risk assessment, due diligence, contract negotiation, and ongoing monitoring and management of third parties.
- Periodically review the assessment process and maintain documentation related to it.
- Support and consult with business units on data classification, vendor assessments, and security reviews.

Third-Party or Vendor Owners (UTHSC Primary Contact for Vendor) and University Units are expected to support Senior Management and follow this policy by:

- Determining the data types, classification, and potential impact on Confidentiality, Integrity, and Availability (with consultation from ITS if needed) which in turn determines which components of the third-party vendor assessment process are recommended or required.
- Assisting with the Planning, Risk Assessment, Contracting, and Monitoring phases of TPRM.
- Notifying the Technology Review Team of intended new or changing third-party relationships which may impact security or its operations.
- Maintaining third-party information within the third-party management system of record.
- Validating the accuracy and content of the services provided by their third parties.
- Completing periodic risk assessment process.
- Issue identification and reporting during any phase of TPRM.

Standard

Initial Screening

All University departments engaging third-party IT products or services are required to undergo a security risk review of the requested product or service. This is accomplished through the UTHSC Classification and Impact Assessment processes. This process is built into the Technology Review Team intake questionnaire.

Based on the security review, the ITS Technology Review Team will determine if a comprehensive security assessment will be required prior to entering into any agreement with the vendor.

Comprehensive Security Assessment

The Third-Party Provider must complete a security questionnaire. Examples include the Higher Education Community Vendor Assessment Toolkit (HECVAT) or Shared Assessments SIG Questionnaire. Additional due diligence may include the Vendor's most recent independent security audit or certification reports (i.e., SOC 2, ISO 27001 certification, HITRUST certification).

The ITS Technology Review Team will review the security assessment and determine whether the Third-Party Provider complies with University security requirements. If the Third-Party Provider is non-compliant, compensating controls will need to be implemented or residual risk will need to be formally acknowledged by the Business Unit.

Contracting Agreements

Third-Party Providers that will store, process, or transmit sensitive or critical Data must:

- Permit the inclusion of the UTHSC Security Addendum as part of the contract where applicable.
- Permit the inclusion of the UTHSC Business Associates Agreement (BAA) as part of the contract where applicable.

  - The BAA provides for "Satisfactory Assurances" per the HIPAA requirements and the "Comprehensive Security Assessment" validates those assurances.
- Permit the inclusion of UTHSC standard security clauses and language in all relevant contracts, which addresses compliance with UTHSC security policies/standards, reporting, performance standards, termination rights, business continuity and contingency, use of subcontractors, limits of liability and indemnification, confidentiality, ownership, destruction or return of data, right to audit, right to access, right to monitor, and compliance with applicable regulations where feasible.

Subsequent Reviews

Security reviews for third-party providers will cover a single use case and are required upon a new solution acquisition, changes in scope or use cases for current solutions, changes in system design or controls, business transfer, merger, or acquisition, and upon the renewal of current solutions.

Periodic review of a Third-Party Provider security posture and continued compliance will be conducted as needed, based upon changes in system use, design or controls, contract renewal or business transfer, merger, or acquisition. Due diligence reviews will be conducted if UTHSC becomes aware of cybersecurity incidents with the third-party provider.

References

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