5.8.18 Third-Party Management of Information Resources

Chapter 5 - Information Technology	Original Effective Date: June 2003
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: June 2018

I. Purpose

To establish policies for all activities involving vendors and third-party information technology providers.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. All vendors and third-party information technology service providers must comply with all applicable UT Health San Antonio (UTHSA) policies.

1. Contracts of any kind, including purchase orders, memoranda of understanding (MOU), letters of agreement, or any other type of legally binding agreement, that involve current or future third-party development, execution, processing or access to Information Resources and/or Data must include terms to ensure that vendors and any subcontractors or other third-parties that maintain, create, or access University Data as the result of the contract comply with all applicable federal and state security and privacy laws and regulations, UTHSA policies, U.T. System policies and standards and must contain terms that ensure that all University Data affected by the contract is maintained in accordance with those policies at all times, including post-termination of the contract.
2. UTHSA procurement staffs, Data Owners and the Chief Information Security Officer (CISO) are jointly and separately responsible for ensuring that all contracts are reviewed to determine whether the contract involves third-party access to

outsourcing, maintenance or creation of University Data and that all such access, outsourcing or maintenance fully complies with UTHSA policies.

3. Any contract involving third-party access to, creation of, or maintenance of Protected Health Information (PHI) must include a Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement (BAA) approved by UTHSA Legal and/or the Compliance Officer.
4. Any contract involving third-party provided credit card services must require that the contractor provides assurances that all subcontractors who provide credit card services pursuant to the contract will comply with the requirement of the Payment Card Industry Data Security Standard (PCI DSS) in the provisioning of the services.
5. Prior to access, maintenance or creation of University Data by a vendor or any other third-party, the Chief Information Security Officer must ensure that an assessment is or has been performed that is designed to ensure that:
    a. the vendor has sufficient technological, administrative and physical safeguards to ensure the confidentiality, security and integrity of the data at rest and during any transmission or transfer; and
    b. any subcontractor or other third-party that will access, maintain, or create data pursuant to the contract will also ensure the confidentiality, security and integrity of such data while it is at rest, during any transmission and physically transferred.
6. As part of the assessment of a vendor or other third-party, the Chief Information Security Officer will request copies of any self-assessments or third-party assessments and audits that the vendor or third-party has access to.
    a. Third-party assessments and audits shall be requested annually for vendors or other third-parties who host or have access to Mission Critical Systems or Confidential Data; and
    b. Periodically as deemed necessary by the Chief Information Security Officer but no less than every three (3) years for all other systems and data.
7. All vendor and third-party network and communication equipment installed on the UTHSA network shall be disabled except when in use for authorized maintenance or other use as defined in the contract.
8. Access controls for vendor and third-party access must be maintained in accordance with all UTHSA policies and standards.
    a. Each vendor or third-party employee with access to UTHSA Information Resources and Data must be approved by the Information Resource Owner. Access rights to information will be based the least privilege principle.
    b. Each vendor must provide UTHSA with a list of all employees working on the contract. The list must be updated and provided to UTHSA within 48 hours of staff changes.

B. **Vendor Contracts**

Vendor must represent, warrant, and certify it will:

1. comply with applicable federal and state laws and regulations and UTHSA policies;
2. hold all Confidential Data in the strictest confidence;
3. limit the use of UTHSA Information Resources and Data only for the purposes of the business agreement;
4. perform reasonable effort to comply with any UTHSA auditing requests, including the auditing of a vendor's third-party or contractor work;
5. not use any UTHSA Data acquired or created in the course of the contract for the vendor's or third-party provider's own purposes or divulged to others other than what is defined in the contract.
6. maintain uniquely identifiable access control and strong password standards to Information Resources and Data;
7. if directly accessing UTHSA Information Resources, comply with applicable polices, standards and procedures for that Information Resource (including, but not limited to Acceptable Use policy and Information Security Awareness Training) using systems that meet minimum UTHSA security configurations;
8. not release any Confidential Data unless vendor obtains UTHSA prior written approval and performs such a release in full compliance with all applicable privacy laws, including the Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA);
9. not otherwise use or disclose Confidential Data except as required or permitted by law;
10. safeguard data according to all commercially reasonable administrative, physical, and technical standards (e.g., such standards established by the National Institute of Standards and Technology or the Center for Internet Security);
11. continually monitor its operations and take any action necessary to assure the data is safeguarded in accordance with UTHSA policies and standards and federal and state laws and regulations;
12. ensure that all software used on UTHSA property is properly licensed for the vendor's and/or third-party's use;
13. comply with vendor access requirements set forth in UTHSA policies and standards;
14. provide written notice of any unauthorized use or disclosure of any Confidential Data within one (1) business day, or if the Information Resource Owner, Procurement Officer, Compliance Officer and Chief Information Security Officer

are satisfied that a longer period is acceptable, within that period, after vendor's or third-party's discovery of such use or disclosure;

15. upon termination of a vendor's employee, contractor or third-party, ensure that all Confidential Data is collected and returned to UTHSA or securely destroyed within 48 hours, provide proof or attestation of that destruction, and immediately surrender all UTHSA identification badges, access cards, equipment and supplies;
16. within 30 days after the termination or expiration of a purchase order, contract or agreement for any reason, vendor must either:
    a. return or securely destroy, as specified by contract or agreement, all data provided to the vendor by UTHSA, including all Confidential Data provided to vendor's employees, subcontractors, agents, or other affiliated persons or institutions, with appropriate proof or attestation; or
    b. in the event that returning or securely destroying the data is not feasible, provide notification of the conditions that make return or destruction infeasible, in which case the vendor or third-party must:
        i. continue to protect all data that it retains;
        ii. agree to limit further uses and disclosures of such data to those purposes that make the return or destruction infeasible for as long as the vendor or other third-party maintains such data; and
        iii. to the extent possible, de-identify such data.

C. **Authority**

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2 "Handbook of Operating Procedures".

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

UT System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 22: Vendor and Third-Party Controls and Compliance

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a timeperiod that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2003	Policy Origination		
06/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edits		