Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.18	**Third-Party Management of Information Resources**	Responsibility:	Chief Information Security Officer

THIRD-PARTY MANAGEMENT OF INFORMATION RESOURCES

Policy

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

A. 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 access to or creation of Information Resources 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, UT Health San Antonio 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.

B. UT Health San Antonio procurement staff, 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 UT Health San Antonio policies.

C. 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 UT Health San Antonio Legal and/or Compliance Officer.

D. 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.

E. 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:

   i. 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

   ii. 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.

F. 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.

   - 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

   - Periodically as deemed necessary by the Chief Information Security Officer but no less than every three (3) years for all other systems and data.

G. All UT Health San Antonio schools, departments, offices and centers engaging vendors, contractors, consultants or other third-party information technology service providers are responsible for managing that relationship, including appropriate termination notifications.

H. All vendor and third-party network and communication equipment installed on the UT Health San Antonio network shall be disabled except when in use for authorized maintenance or other use as defined in the contract.

l. All remote vendor or third-party access to the UT Health San Antonio network or other Information Resource must use a secured access method approved by the Chief Information Security Officer and comply with all UT Health San Antonio Access Control policies, standards and procedures.

- Each vendor or third-party employee with access to UT Health San Antonio sensitive information must be approved by the data owner (Principal Investigator, Access Control Executive, department head, etc.) to handle that information. Access to information will be based the least privilege principle for the responsibilities assigned to the employee.

- Each vendor must provide UT Health San Antonio with a list of all employees working on the contract. The list must be updated and provided to UT Health San Antonio within 48 hours of staff changes.

Vendor Contracts

Vendor must represent, warrant and certify it will:

a. comply with applicable federal and state laws and regulations and UT Health San Antonio policies;

b. hold all Confidential Data in the strictest confidence;

c. limit the use of UT Health San Antonio Information Resources and Data only for the purposes of the business agreement;

d. perform reasonable effort to comply with any UT Health San Antonio auditing requests, including the auditing of a vendor's third-party or contractor work;

e. not use any UT Health San Antonio 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.

f. maintain uniquely identifiable access control and strong password standards to Information Resources and Data;

g. if directly accessing UT Health San Antonio 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 UT Health San Antonio security configurations;

h. not release any Confidential Data unless vendor obtains UT Health San Antonio 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);

i. not otherwise use or disclose Confidential Data except as required or permitted by law;

j. 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);

k. continually monitor its operations and take any action necessary to assure the data is safeguarded in accordance with UT Health San Antonio policies and standards and federal and state laws and regulations;

l. ensure that all software used on UT Health San Antonio property is properly licensed for the vendor's and/or third-party's use;

m. comply with vendor access requirements set forth in UT Health San Antonio policies and standards;

n. provide written notice of any unauthorized use or disclosure of any Confidential Data within one (1) business day, or if the Data Owner, 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;

o. upon termination of a vendor's employee, contractor or third-party, ensure that all Confidential Data is collected and returned

to UT Health San Antonio or securely destroyed within 48 hours, provide proof or attestation of that destruction, and immediately surrender all UT Health San Antonio identification badges, access cards, equipment and supplies;

p. within 30 days after the termination or expiration of a purchase order, contract or agreement for any reason, vendor must either:

i. return or securely destroy, as specified by contract or agreement, all data provided to the vendor by UT Health San Antonio, including all Confidential Data provided to vendor's employees, subcontractors, agents, or other affiliated persons or institutions, with appropriate proof or attestation; or

ii. 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:

- continue to protect all data that it retains;
- 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
- to the extent possible, de-identify such data.

Authority

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

References

- U.T System Policy 165 Standard 22