UTEP Standard 22: Vendor and Third-Party Controls and Compliance

UTEP recognizes that Vendors and other contractors serve an important function in the development and/or support of services, hardware, and software, and in some cases, the operation of computer networks, servers, and/or applications. This standard applies to contracts entered into by UTEP that involve access or creation of information resources or University data by a third party.

22.1 Contracts. Contracts of any kind, including purchase orders, memoranda of understanding (MOU), letters of agreement, or any other legally binding agreements that involve access, maintenance, or creation of information resources or data by a third party, must include terms determined by UT System Office of General Counsel (OGC) or UTEP Office of Legal Affairs to be sufficient for ensuring that vendors, subcontractors, or other third parties who maintain, create, or access University data pursuant to the contract, shall comply with all applicable federal and state security and privacy laws, the UTEP Information Resources Use and Security Policy and Standards, and all applicable U.T. System Policies or Standards, including UTS 165. Such contracts must include terms which ensure that University data is maintained in accordance with this standard at all times, including post-termination of the contract.

22.2 The Data Owner, UTEP procurement officers and staff, and 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, outsourcing, maintenance, or creation of University data; and that all such access, outsourcing, maintenance, or creation of University data fully complies with this Standard at all times.

22.3 Any contract involving third-party access, creation, or maintenance of Protected Health Information (PHI) as defined in 45 C.F.R. § 164.501, must include a Health Insurance Portability and Accountability Act (HIPAA) business associate agreement in a form approved by UTEP or OGC counsel.

22.4 Any contract involving third-party-provided credit card services must require the Contractor to provide assurances that all subcontractors who provide credit card services pursuant to the contract will comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) in their provision of services.

22.5 Vendor or other Third-Party Assessment. Prior to access, maintenance, or creation of University data by a Vendor or other third party, UTEP must ensure that an assessment is or has been performed 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 the data at rest and during any transmission or transfer.

22.6 As part of the University's assessment of a Vendor or other third party, the University will request copies of all self-assessments or third-party assessments that the Vendor or third party has access to.

22.7 Access Control Measures. The University must control Vendor and other third-party access to its data based on data sensitivity and risk. Access control measures must incorporate the following:

(a) Vendor must represent, warrant, and certify it will:

i. hold all Confidential Data in the strictest confidence;

ii. not release any Confidential Data unless Vendor obtains the University's prior written approval. Vendor may be required to protect or disclose data in compliance with applicable privacy laws, including but not limited to the Family Educational Rights and Privacy Act (FERPA);

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

iv. safeguard Data according to all commercially reasonable administrative, physical, and technical Standards (e.g., such Standards established by the Nation Institute of Standards and Technology or the Center for Internet Security);

v. continually monitor its operations and take any action necessary to ensure that the Data is safeguarded in accordance with the terms of UTEP Information Resources Use and Security Policy and Standards; and

vi. comply with the Vendor access requirements that are set forth in this Standard.

22.8 Breach Notification. The following shall be required from the Vendor.

(a) If an unauthorized use or disclosure of any Confidential Data occurs, the Vendor must provide:

i. written notice within one business day after Vendor's or third-party's discovery of such use or disclosure; and

ii. all information that UTEP may request concerning such unauthorized use or disclosure.

22.9 Return of Data. 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 the University, including all Confidential Data provided to Vendor's employees, subcontractors, agents, or other affiliated persons or institutions; or

(b) if returning or securely destroying the Data is not feasible, then Vendor shall provide notice 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 use or disclosure of the Data to those purposes that made its return or destruction infeasible for as long as the Vendor or third party maintains the Data; and

iii. to the extent possible, de-identify the Data.

22.10 Revision History

Created: May 31, 2017 (to align with UTS165)
Revised: June 13, 2019 (update broken links and compliance language)
Approved: June 13, 2019
Gerard D. Cochrane Jr., Chief Information Security Officer