UTEP Standard 10: Risk Management

The purpose of Risk Management is to empower the ISO to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

10.1 An accurate inventory of Information Resources and Identified Owners will be maintained by UTEP Inventory Department and provided to the ISO.

10.2 Information Resources Owners. For Information Resources under the Owners' authority, Owners must, in consultation with the UTEP CISO:

(a) define, approve, and document acceptable Risk levels and Risk mitigation strategies; and

(b) conduct and document Risk assessments to determine Risk and the inherent impact that could result from their unauthorized access, use, disclosure, disruption, modification, or destruction. timing of assessments shall be:

i. annually for all Mission Critical Information Resources and Information Resources containing Confidential Data; and

ii. at periodic time intervals to be defined by the Resource Owner in consultation with the CISO for non-Mission Critical Information Resources and Information Resources not containing Confidential Data.

10.3 Information Resources Custodians. Custodians of Mission Critical Information Resources must implement approved Risk mitigation strategies and adhere to Information Security Policies and Procedures to manage Risk levels for Information Resources under their care.

10.4 Chief Information Security Officer (CISO). CISO must ensure that annual Information Security Risk assessments are performed and documented by each Owner of Mission Critical Information Resources or Information Resources containing Confidential Data.

10.5 Sponsored Projects. Principal Investigators (PIs) must perform security assessments, in collaboration with the Office of Sponsored Projects and the UTEP CISO, of the implementation of required security controls (i.e., control objectives, controls, Policies, processes, and Procedures for Information Security) for sponsored projects under their authority. Security assessments for sponsored projects must be performed annually based on Risk.

10.6 Risk Assessment of Third-Party Service Providers. A third-party Risk assessment is required in the following situations:

(a) when purchasing services that result in exchange of Confidential University Data or hosting of Confidential University Information Resources with a Vendor or other organization; or

(b) when purchasing systems or software, whether it is to be hosted on premises or at a Vendor facility, if Confidential University Data will be stored within or processed by the system or software. For additional requirements please refer to Standard 4: Access Management.

10.7 Information Security Risk Assessments. Information Security Risk Assessments that are to be aggregated for system-wide reporting to the U. T. System Executive Compliance Committee and/or the U. T. System Board of Regents shall be conducted using a risk management framework and process defined by U. T. System Office of Information Security and shall be coordinated at the Institutional level by the CISO.

10.8 Risk Acceptance. Decisions relating to acceptance of Risk must be documented and are to be made by:

(a) the Information Resource Owner, in consultation with the CISO or designee, for resources having a residual Risk or Low or Moderate.

(b) the Chief Administrative Officer, or designee, considering recommendations of the Owner and CISO, for resources having a residual Risk of High.

10.9 Revision History

First Draft: May 12, 2017 (based on new UTS165)
Approved: May 12, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer