UTEP Standard 3: Information Security Program

3.1 Information Security Program Requirement. Each Institution and any governing body with oversight for Common Use Infrastructures must establish and maintain a Security Program that includes appropriate protections, based on risk, for all Information Resources, including outsourced resources, owned, leased, or under the custodianship of any governing body or department, operating unit, or employee of the Institution.

3.2 Information Security Program. Each Security Program must include and document the following:

(a) annual risk assessment;

(b) current inventory of

i. institution-owned or managed devices deployed throughout the institution, and

ii. Mission-Critical applications and applications containing Confidential Data;

(c) strategies to address identified risks to Mission Critical Information Resources and Confidential Data;

(d) annual action plan, training plan, and monitoring plan; and

(e) metrics, reports, and timelines established by the U. T. System Office of Information Security Compliance.

3.3 Collection of Information Security Metrics. Each Institution must collect required metrics data in ways that are documented and verifiable.

3.4 Information Security Program Exceptions. The Owner of the Information Resource and the ISO must document and justify any exceptions to specific program requirements in accordance with requirements and processes defined in UTEP Standard 23 – Security Control Exceptions and UTEP ISO Security Exception Reporting Process.

3.5 Revision History

First Draft: May 12, 2017
Approved: May 12, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer