UTEP Standard 21: System Development and Deployment

21.1 Information Security Consideration. UTEP must adopt Institutional Polices, Standards, Guidelines, and/or Procedures to ensure that the protection of Information Resources (including Data confidentiality, integrity, and availability) is considered during the development or purchase of new Information Systems or services. For more information and additional requirements that must be followed for all applications and systems processing Confidential Data please refer to The University of Texas at El Paso Minimum Security Standards for Systems, The University of Texas at El Paso Minimum Security Standards for Applications Development and Administration, and The University of Texas at El Paso Payment Card Industry (PCI) Data Security Standard (DSS).

21.2 Redundant Information Systems or Services. Information Systems that duplicate services provided by the UTEP Enterprise Computing (EC) group are discouraged because they increase opportunity for exposure of Data. The Information Resources Manager (IRM) shall approve the purchase or deployment of new Decentralized IT Information Systems or services (e.g., electronic mail/web/file servers, file/system backup, storage, etc.) that duplicate applications or services provided by EC. The Owner of the duplicative Information System, working with the IRM, must document and justify exceptions based on business need, weighed against Risk of potential unauthorized access or loss of Data.

21.3 Required Controls. The University must ensure that controls for the protection of Information Resources (including Data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications. The following procedures are required:

(a) All associated systems and applications must restrict access and provide methods for appropriately restricting privileges of authorized users. User access to applications is granted on a need-to-access basis;

(b) Separate production and development or test environments will be maintained to ensure the security and reliability of the production system. Whenever possible, new development or modifications to a production system will be made first in a test environment. These changes should be thoroughly tested for valid functionality prior to being released into the production environment;

(c) Performing a security assessment prior to the purchase of any new information security services that receive, maintain, and/or share Confidential Data;

(d) Including vulnerability assessments and code scans to the Information Systems development cycle;

(e) Performing a vulnerability assessment and including a static or dynamic code scan of all new web applications prior to moving them to production;

(f) Information technology outsourced contracts must address security, backup, and privacy requirements, and should include a provision for UTEP to conduct a security assessment or a right to review security assessments performed by third parties, or other provisions to provide appropriate assurances that applications and Data will be appropriately protected when Confidential Data is involved. Vendors are required to adhere to all Federal and State laws as well as Regent's Rules pertaining to the protection of Information Resources and the privacy of Confidential Data.

21.4 Security Review and Approval. The UTEP Chief Information Security Officer (CISO) must review and approve security requirements, specifications, and, if applicable, third-party Risk Assessments for any new computer hardware, software, applications, or services that are Mission Critical or that receive, maintain, and/or share Confidential Data.

21.5 IT Systems Contracts. Contracts for purchase or development of automated systems that are associated with Confidential Data must address security, backup, and privacy requirements, and should include a right for UTEP to conduct a security assessment or a right to review security assessments performed by third parties and other provisions to provide appropriate assurances that applications and Data will be adequately protected.

21.6 Revision History

Created: May 31, 2017 (to align with UTS165)
Approved: June 16, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer