UTEP Security Program and Data Classification Standard, and UTS165 and its

(a) Data Systems that house Confidential University Data,

(b) Credit card information must be protected in accordance with

(c)

secret password or PIN that is kn

(f) Accounts and passwords must n

(g)

(h)

(i)

(j)

(k)

).

(l)

data. All personally owned computers, mobile devices, USB thumb drives, or similar devices must be Password protected and

(a) Identification and Transmission of the least amount of Confidential Data required to achieve the intended business objective;

(b) All Confidential Data transmitted over the Internet must be appropriately encrypted;

(c) Confidential Data transmitted between Institutions and Shared Data Centers must be appropriately encrypted;

(d) Confidential Data transmitted or received must be deleted upon completion of the intended business objective unless otherwise subject to records retention, in which case it must be encrypted or password protected.

11.6 Protecting Common Use Information Resources

(a) The ISO is responsible for implementation of an Information Security Program for Common Use Infrastructures, and for documenting associated roles and responsibilities.

(b) For services provided via Common Use Infrastructures, Memorandum of Understanding (MOU) documents between U.T. System and host Institutions and between UTEP and participant Institutions must identify roles and responsibilities for provision of Information security controls.

11.7 Discarding Electronic Media. UTEP must discard electronic devices and media containing University Data:

(a) in a manner that adequately protects the confidentiality of the Data and renders it unrecoverable, such as overwriting or modifying the Electronic Media to make it unreadable or indecipherable or otherwise physically destroying the Electronic Media. Please refer to the UTEP Electronic Data Destruction Guidelines; and

(b) in accordance with the applicable UTEP Records Retention Schedule.

11.8 Related Policies, Standards, Procedures, Guidelines and Applicable Laws

- UTEP Information Resources Use and Security Policy
- Standard 2: Acceptable Use of Information Resources
- UTEP Minimum Security Standards for Systems
- UTEP Electronic Data Destruction Guidelines
- Security Exception Reporting Process
- Records and Information Management
- Texas Administrative Code 202

- x UT System UTS-165
- x European Union General Data Protection Regulation (EU GDPR)
- x NIST SP 800-171 Revision 1

11.9 Revision History

Complete Rewrite: May 5, 2017
Reviewed: June 7, 2018
Provide additional guidelines [11.1(m)] and policies applicable to portable computing devices; include Controlled University Data [11.3(b-c)]; add reference links to CUI and GDPR
Approved: May 5, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer
Approved: June 14, 2018 by CISO