UTEP Standard 11: Safeguarding Data

11.1 UTEP Policies, Standards, and/or Procedures must describe and require steps for protecting University Data using appropriate administrative, physical, and technical controls in accordance with UTEP's Information Security Program and Data Classification Standard, and UTS165 and its associated Standards.

(a) Data Owners must maintain an inventory and have documentation of all systems that house Confidential University Data;

(b) Credit card information must be protected in accordance with Payment Card Industry Digital Security Standards (PCI DSS). NOTE: Any transmission of credit card information unencrypted or through email is strictly prohibited;

(c) Confidential documents must not be left in easy to access areas, such as leaving documents or computer equipment on desks that unauthorized individual(s) can view or remove. Make sure that you lock and secure all areas when you leave your office;

(d) Computing devices left ON while unattended shall have a screen saver enabled that is password-protected and adheres to the University minimum password requirements;

(e) Access to Confidential University Data on computing devices and/or servers must require a combination of a unique login and a secret password or PIN that is known only by the authorized user;

(f) Accounts and passwords must not be shared under any circumstances;

(g) Storage of Confidential University Data on electronic media must be encrypted or password protected;

(h) Confidential University Data may not reside on devices that do not adhere to the system security standards established by the University;

(i) Confidential University Data may not be transported outside of the United States without the prior approval of the Information Security Office (ISO);

(j) Accounts that give users access to Information Resources must be used only by the person whom the account is assigned;

(k) All passwords used to access Confidential University Data on any computing device must meet the minimum password complexity standards set by University Policy (see Standard 15: Passwords).

(l) Unattended portable computing devices must be physically secure. This means that they must be locked in an office, locked in a desk

drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

(m) Purchase of portable storage devices must include encryption technology compatibility with University encryption standards and policies. All Confidential or Controlled University Data that is stored or transported on portable media must be encrypted in accordance with University policies. Security Exceptions to this policy must be submitted to the Chief Information Security Officer for approval.

11.2 Third-Party Service Providers Storing University Data. University Data must not be stored on personally procured third-party (e.g., Cloud) storage services. All third-party services storing University Data must have a valid contract in place that has been signed by the UTEP Purchasing Office.

11.3 Password and Encryption Protection for Computing Devices and Data.

(a) Desktop Computers.

i. All High Risk Desktop Computers owned, leased, or controlled by the University must be Password protected and encrypted using methods approved by the Chief Information Security Officer;

ii. All desktop computers purchased after September 1, 2013 must be Password protected and encrypted, regardless of data classification, using methods approved by the CISO before their deployment.

(b) Laptop Computers and Other Portable Computing Devices.

i. All laptop computers and other portable computing devices, including but not limited to mobile and smart phones, and tablet computers, that are owned, leased, or controlled by the University, must be encrypted, regardless of data classification, using methods approved by the CISO.

ii. USB thumb drives and similar removable storage devices owned, leased, or controlled by the University must be encrypted, using methods approved by the CISO, before storage of any Confidential or Controlled University Data on the device.

(c) Personally Owned Devices. Specific permission must be obtained from the Department Head, Chair or Dean AND the CISO before a user may store Confidential or Controlled University Data on any personally owned computers, mobile devices, USB thumb drives, or similar devices. Such permission should be granted only upon demonstration of a business need and an assessment of the risk introduced by the possibility of unauthorized access or loss of the

data. All personally owned computers, mobile devices, USB thumb drives, or similar devices must be Password protected and encrypted using methods approved by the CISO if they contain any of the following types of University Data:

i. Information made confidential by Federal or State law, regulation, or other legally binding order or agreement;

ii. Federal, State, University, or privately sponsored Research that requires confidentiality or is deemed sensitive by the funding entity; or

iii. any other Information that has been deemed by UTEP as essential to the mission or operations of UTEP to the extent that its Integrity and security should be maintained at all times.

(d) Approved Encryption Methods are published and maintained by the UTEP Information Security Office.

(e) Exceptions must be filed with the Information Security Office in the event of hardware compatibility conflicts, technology limitations for certain types of devices, etc. All exceptions must note why alternative solutions are not possible (newly purchased hardware should be selected to adhere to UTEP standards prior to purchase) and identify the compensating controls that will be implemented to offset the risk created by the lack of encryption. A single exception may be filed for a number of devices as long as the devices can be uniquely identified (e.g., UTEP Inventory Tag Number, Serial Number, MAC Address).

11.4 Assured Access to Encrypted Data

(a) University Owned, Leased, or Controlled Devices - data and device owners are responsible for ensuring that encrypted data will be accessible in the event decryption keys or related credentials become lost or forgotten and no other copy of the data is available. Only escrow methods approved by the CISO are permissible.

(b) Personally Owned Devices - for personally owned devices, the device owner is responsible for ensuring that encrypted Data is backed up to University owned or sanctioned storage using processes prescribed by the CISO.

11.5 Protecting Data in Transit. Data Owners shall implement appropriate administrative, physical, and technical safeguards to adequately protect the security of Data during transport, including electronic transmission. The following shall all be addressed:

(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

- UT System UTS-165
- European Union General Data Protection Regulation (EU GDPR)
- 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