29.01.03.C2.28 Classification and Protection of Data; Encryption
Approved June 25, 2012
Supplements University Rule 29.01.03.C2

1. GENERAL

The Texas Administrative Code (“TAC”) §202.71(b) requires institutions of higher education to define data classification categories and to establish appropriate controls for each category. Those controls typically include user authentication, encryption, periodic scanning, and the sanitization of decommissioned or repurposed storage media. This Procedure defines the classification of University data, and the controls to be implemented to protect University data.

2. APPLICABILITY

This Procedure applies to all University employees and affiliates, including contractors. It addresses encryption requirements and controls for confidential and/or university-sensitive data that is at rest (including portable devices and removable media) regardless of ownership of the particular storage device, and data in motion (transmission security). This Procedure is compatible with, but does not supersede or guarantee compliance with all State and federal encryption standards.

The purpose of the implementation of this procedure is to provide a set of measures that will mitigate information security risks associated with the use of sensitive and university-sensitive data. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also see Procedure 29.01.03.C2.25 – “Exceptions to Risk Mitigation Measures.”

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions. The definitions below apply only to this document.

Sanitize means to overwrite data on a storage device with a program that complies with Department of Defense standard 5220.22-M.

4. PROCEDURES

4.1. Data Classifications. The University has defined the following data classifications:
(1) **Confidential**: Data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act) and other constitutional, statutory, judicial, and legal agreements. Examples of “Confidential” data include but are not limited to:

a. Personally Identifiable Information (“PII”), such as: a name in combination with Social Security Number (SSN) and/or financial account numbers;

b. Student Education Records;

c. Information protected by a legal agreement (e.g., a non-disclosure agreement);

d. Medical Records.

(2) **University-Sensitive**: Data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection. Examples of university-sensitive data may include but are not limited to:

a. operational information;

b. personnel records;

c. information security procedures;

d. research;

e. internal communications.

(3) **Public**: Information intended or required for public release as described in the Texas Public Information Act.

4.2. **Responsibilities of All Users Regarding the Storage and Transmission of Confidential and University-Sensitive Information.**

(1) Users should constantly strive to minimize 1) the amount of confidential and university-sensitive information stored on all their computing devices and 2) the transmission of such information to other parties.

(2) Owners of confidential or university-sensitive data shall only grant access
to that data to authenticated users. In other words, unauthenticated or “public” access to confidential or university-sensitive data shall not be permitted.

(3) Confidential and university-sensitive data should not be stored on a portable computing device (e.g., laptop, smartphone, USB storage device) or a non-University computing device (e.g., home workstation, Internet host) unless absolutely necessary.

(4) If confidential or university-sensitive data must be stored on a portable or non-University computing device, that data must be encrypted. (Note: for a given portable or non-University-owned computing device, this requirement can be satisfied by the use of whole-disk encryption (e.g., BitLocker) on the portable or non-University computing device.)

(5) Neither confidential data nor unencrypted university-sensitive data shall be stored in a location that either 1) permits unauthenticated access to the data or 2) is accessible by a server, the primary purpose of which server is to provide anonymous or unauthenticated access to data (e.g., a web server serving up public web pages).

(6) If confidential or university-sensitive data must be transmitted over a non-University-owned network, either 1) the data itself shall be encrypted, 2) the link shall be encrypted (e.g., VPN, HTTPS, Secure FTP), or 3) both the data and link shall be encrypted.

(7) Before confidential or university-sensitive data is transferred to another institution of higher education, contractor, or other third party, that third party must affirm that they will protect the transferred data in accordance with the conditions imposed by the data’s Owner, which conditions will contain, at a minimum, the conditions specified in this Procedure.

4.3. Custodians’ Responsibilities re Scanning and Reporting.

(1) At least once a year, Custodians shall scan their information resources for specific types (e.g., social security numbers) of confidential and/or university-sensitive data, which types will be specified in supplemental guidelines.

(2) Custodians shall keep logs of those scans and share those logs with the Information Security Office.

(3) Within a reasonable time after the performance of a scan, Custodians shall affirm in writing to the Information Security Office that the data stored on the scanned information resource does or does not comply with section 4.2
above. If the data on the scanned information resource does not comply, the Custodian must bring the data into compliance within a reasonable amount of time.

(4) At least once a year, Custodians shall classify the data stored on the information resources for which they are responsible, and report that classification in the annual information security risk assessment process.

4.4. Custodians’ Responsibility to Sanitize Storage Media. When University storage media is de-commissioned or repurposed, the Custodian of that University storage media shall ensure that the media is either 1) sanitized, or 2) physically destroyed, e.g., by shredding.


(1) All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, AES 128-bit encryption.

(2) The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed and approved by the CIO or his or her designee(s).

(3) Recovery of encryption keys must be part of business continuity planning.

5. CONSEQUENCES FOR VIOLATIONS

All University employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Any device, system, or software found in violation of this procedure may be disconnected from the University Network.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct
Texas A&M University-Corpus Christi Rule
   o 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
   o 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation:  Information Security Officer

Office of Responsibility:  Office of the Associate VP for Information Technology and CIO