The Division of Information Technology
University Information Security Standards

Information Security Standard – Data Classification (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Data Classification provides a framework for managing data assets based on value and associated risks. It also guides the application of the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All data, whether electronic or printed, should be classified. Consistent use of data classification reinforces with users the expected level of protection of those data assets in accordance with West Texas A&M Security Rules and information security standards.

The purpose of this standard is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security controls and requirements may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

2. Applicability

This applies to all University Data owners, custodians, and users. It also applies to information resources storing University Data regardless of ownership of the particular storage device. Other Federal, State, or contractual requirements may be in addition to or supersede the requirements specified in this standard.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with Internet/Intranet use. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with **Texas Administrative Code 202 - Information Security Standards**, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk

management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all users of University information resources.

3. Responsibility

The owner of an information resource, with the concurrence of the President or Chief Information Officer, is responsible for classifying business functional information. The University is responsible for defining all information classification categories except the "Confidential" category.

It is the responsibility of anyone (e.g., owner, custodian, user) having data in their possession or under their direct control (e.g., manages the storage device) to know the classification of the data and ensure the appropriate safeguards are in place. Anyone possessing confidential data shall ensure that appropriate risk mitigation measures (e.g., encryption) are in place to protect data from unauthorized exposure.

4. Definitions

4.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Examples of "Confidential" data may include, but are not limited to:

(1) Personally identifiable information such as a name in combination with social security number (SSN) and/or financial account numbers

(2) Student education records

(3) Intellectual Property such as copyrights, patents, and trade secrets

(4) Medical records

4.2 Custodian: Responsible for implementing owner-defined controls and access to an information resource. Custodians may include West Texas A&M University employees (faculty and staff), vendors, and any third party acting as an agent of or otherwise on behalf of West Texas A&M University and/or the owner.

4.3 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax

machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

4.4 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

4.5 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4.6 Public: (default classification) information intended or required for public release as described in the Texas Public Information Act.

4.7 Sensitive: An optional West Texas A&M University or owner defined category. Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection. Examples of sensitive data may include, but are not limited to the following:

(1) Operational information
(2) Personnel records
(3) Information security procedures
(4) Research
(5) Internal communications

4.8 Specialized Information System: Systems containing embedded information technology that have been assigned a very specific task (e.g. instruments with embedded computer systems). The following information systems do not need to be documented or scanned:

(1) Printers
(2) Scanners
(3) Fax Machines

4.9 University Data: Data or information that is in the possession or under the control of an individual (i.e. owner, custodian, or user) by virtue of that person's employment or affiliation with the university.

4.10 User of an Information Resource: An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

4. Procedures

4.1 Data is to be classified as Confidential and/or Mission Critical, Sensitive, or Public (default). The classification of the electronically stored data is to be reported in the annual information security risk assessment process.

4.2 Access to confidential or sensitive information shall not be permitted with the use of a user ID alone (e.g. UIN only).

4.2 Where feasible, all data files are to be scanned on an annual basis to determine if those files contain SSN's. If SSN's are found or known to be present in a file, they are to be removed or appropriate risk mitigation measures applied if their continued presence is required. The results of the file scanning and risk mitigation measures taken shall be reported during the annual risk assessment process. All SSN's that are to be retained and stored are to be reported to and approved by the division/department head. The reporting and approval process will be in the manner indicated in the risk assessment process. Specialized information systems that cannot be scanned and or not capable of storing SSN's shall also be documented accordingly as part of the risk assessment process.

5. Exclusions

5.1 A file is not subject to the requirements in 4.3 if the only social security number(s) contained in the file belong to the owner and custodian of the file or his/her immediate family members.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer