Texas A&M University System Data Classification Standard (DRAFT v1.2)

STANDARD

The Texas A&M University System (A&M System) Data Classification Standard consists of four specific data classifications based on fit within a spectrum indicating the degree to which access to data may be openly available or must have restricted access. While the intent is to define the different types of information and how they should be secured, it is also the intent to make it as simple and straightforward as possible. These four classifications are:

Classification	Description	Examples	Comments
Regulated Information/data	This category focuses on information that is regulated by federal statute or through third-party agreements, which may include covenants.	Data that meets the definition of SPI under the Texas Business and Commerce Code 521.002(a)(1) and 521.002(a)(2): HIPAA Security (45 CFR Parts 164), PCI DSS v2.0, FTI, FICA, tax information • Patient billing information and protected health information as protected by HIPAA. • Student education records. These are protected by FERPA. • Some research information, such as that which is controlled by a covenant or third-party agreement, may be subject to this classification	HIPAA, FTI or PCI information is covered in this category. Also, it may include agreements or contracts for research work.
Confidential Information/data	The Confidential classification is defined by the DIR in TAC §202.1 Subchapter A as, "Information 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 agreement requirements)."	• Computer vulnerability reports • Credit Card numbers associated with an individual's name. (PCI)Social security number associated with a person's name.	Information (data), cannot simply be declared to be "Confidential." This classification is reserved for information that is protected from public release based on state or federal law, or binding judicial or legal agreement. Likewise, data cannot be declared to be "Confidential" under all circumstances. Context is an essential element. (In terms of the Federal Standards for Security Categorization of Federal Information and Information Systems , FIPS 199, this category equates to HIGH IMPACT for a Confidentiality breach)
Controlled (Sensitive) Information/data	The Controlled classification applies to information/data that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through	Operational records. Operational statistics. Employee salaries. Budgets, Expenditures, Internal communications that do not contain confidential information. General research data.	This classification likely encompasses that greatest volume of data within the University. (In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality

	request via the Texas Public Information Act or similar state or federal law.		breach)
Public Information/data	Public information/data includes all data made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information/data for which public disclosure is intended or required.	Published system and system member policy documents, organizational charts, Statistical reports, Fast Facts, unrestricted directory information, educational content available to the public at no cost.	Information can migrate from one classification to another based on information life-cycle. For example, a draft policy document would fit the criteria of "Controlled Information" until being published upon which it would become Public Information. (In terms of FIPS 199, this category equates to LOW IMPACT for a Confidentiality breach.)

1. Each member institution or agency must establish a Member Data Classification Standard. The member may adopt the A&M System Data Classification Standard or may create a different Member Standard. However all data classifications established in a Member Standard must correspond to one of the A&M System data classifications. All Member Data Standards must include the confidential classification category.
2. The A&M System Data Classification Standard will be used to assess data access and security requirements for data to be stored or processed within member shared data centers.

3. When determining security controls to use for a given set of data, Data Owners and Custodians should also assess whether special requirements exist regarding importance of data availability and integrity and rate the need as LOW, MODERATE, or HIGH for both integrity and availability. The needs regarding availability and integrity may impact security control decisions, but are not used for purposes of assigning a classification label of Confidential, Controlled, or Published.

BACKGROUND

The Business Requirement:

A&M System members collect, create, process, store, and communicate information (data), to achieve System missions of instruction, research, patient care, and public service. Based on its nature, purpose, sensitivity, time criticality, and regulatory requirements, information is managed to preserve appropriate levels of confidentiality, integrity, and, availability. Data classification is an important input for making data management decisions. As Texas public institutions of higher education, A&M System members must adhere to Texas State data classification requirements. For academic research and business reasons, the A&M System must also align with federal data classification requirements.

State of Texas Requirement:

The State of Texas mandates that institutions of higher education classify data. Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, Subchapter C, Rule §202.70 states in part, "Information resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. These assets shall be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to state information resources shall be appropriately managed."

TAC 202, Rule §202.71 (b) then states, "Institutions of higher education are responsible for defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, and establishing the appropriate controls for each."[1]

Federal Requirement:

The E-Government Act of 2002 (Public Law 107-347), recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked the National Institute of Standards and Technology (NIST) with responsibilities for standards and guidelines, including the development of Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.[2]

Federal Information Processing Standard 199 (FIPS 199) and FISMA have particular importance to institutions of higher education because federal agencies and granting authorities are increasingly requiring compliance with FISMA, including the data classification requirements, as condition of grant award. Ability to demonstrate adherence with principles of FISMA provides competitive advantage to TAMUS members in the pursuit of research.

The FIPS 199 Data Security Framework:

The FIPS 199 Framework consists of a matrix that provides an assigned security category based on level of risk (impact x likelihood of occurrence) for each of the security domains of Confidentiality, Integrity, and Accessibility, as shown in the following diagram:

[1] Confidential Information--Information 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 agreement requirements).

[2] FIPS Publication 199, Page 1, FIPS Publication 199 addresses the first task—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government promotes (1) effective management and oversight of information security programs.

	POTENTIAL IMPACT		
Security Objectives	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restriction on information access and disclosure including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information would be expected to have **no or only slight** adverse effect on organization operations, organization assets, or on individuals.	The unauthorized disclosure of information would be expected to have **limited** adverse effect on organization operations, organization assets, or on individuals.	The unauthorized disclosure of information would be expected to have a **severe or catastrophic** adverse effect on organization operations, organizational assets, or on individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information would be expected to have **no or only slight** adverse effect on organizational operations, organizational assets, or on individuals.	The unauthorized modification or destruction of information would be expected to have **limited** adverse effect on organization operations, organizational assets, or on individuals.	The unauthorized modification or destruction of information would be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or on individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system would be expected to have **no or only slight** adverse effect or organizational operations, organizational assets, or on individuals.	The disruption of access to or use of information or an information system would be expected to have **limited** adverse effect or organizational operations, organizational assets, or on individuals.	The disruption of access to or use of information or an information system would be expected to have **severe or catastrophic** adverse effect or organizational operations, organizational assets, or on individuals.

Using the table above, any particular set of data can be assigned three security ratings, one for Confidentiality (LOW, MODERATE or HIGH), another for Integrity (LOW, MODERATE or HIGH), and a third for Availability (LOW, MODERATE or HIGH). This is useful for defining security controls, because a set of data that may have low need for confidentiality, (LOW Impact) but require HIGH availability. For such data, encryption may not be appropriate, but redundancy may be a requirement. Most breaches that cause HIGH impact are result of unauthorized access to Confidential information. Therefore, ***the A&M System's Data Classification Standard and assignment of classification places prime importance on the level of Confidentiality required of the data.***