# Texas A&M University System Data Classification Standard

The Texas A&M University System (A&M System) Information Classification Standard consists of three specific classifications based on access restrictions and risk. This classification standard applies to all members. While the classification applicable to specific information may change based on circumstances, the intent of this standard is to define the appropriate classification for different types of information. These three classifications are:

| Classification | Description | Examples | Comments |
|---|---|---|---|
| **Confidential Information** | Information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements.<br><br>This category also focuses on information that is restricted through certain legal agreements. | • Patient billing information and protected health information as protected by HIPAA.<br><br>• Student education records protected by FERPA.<br><br>• Classified National Security information under Executive Order 13526. The higher standard of NIST and federal regulations that applies to this data should be in force. The Facility Security Officer (FSO) should be consulted when a National Security Information is concerned.<br><br>• Information/Information System security plans, reports and related information<br><br>• Credit/debit card numbers, bank account numbers<br><br>• Personal financial information<br><br>• Social security numbers<br><br>• A&M System intellectual property and research information having commercial potential<br><br>Confidential Information requiring breach notifications or having stricter access requirements may include: SPI as defined by Texas Business and Commerce Code § 521.002(a)(2); credit card numbers covered by PCI DSS v3.1. | This classification is reserved for information that is protected from public release based on state or federal law or binding legal agreement.<br><br>This classification may not be absolute; context is an essential element.<br><br>Owners of confidential information must ensure such information is correctly classified.<br><br>Custodians of confidential information must implement appropriate controls.<br><br>(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)<br><br>HIPAA, FTI or PCI information is covered in this category. This classification may include agreements or contracts for research work that require higher levels of security and/or procedural elements for handling of information.<br><br>Consult the Office of General Counsel regarding confidential information requested through open records, subpoena, or other legal process. |

| | | | |
|---|---|---|---|
| **Controlled Information** | Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws. | This information includes institutional budgetary, financial and operational records such as expenditures, statistics, contracting information, non-confidential personnel information. It may also include non-confidential internal communications.<br><br>General research information falls into this classification if it is Controlled Unclassified Information (CUI). CUI protection as defined by Presidential Executive Order 13556 related to the security of nonfederal information systems is applicable. | This classification encompasses that greatest volume of information within the University and also contains the Controlled Unclassified Information (CUI) designation.<br><br>(In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality breach)<br><br>Consult the Office of General Counsel regarding controlled information requested through open records, subpoena, or other legal process. |
| **Public Information** | Public information includes all information 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 for which public disclosure is intended or required. | Published system and system member policy documents, organizational charts, Statistical reports, Fast Facts, unrestricted directory information, employee salaries, and 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.<br><br>(In terms of FIPS 199, this category equates to LOW IMPACT for a Confidentiality breach.) |

1. Each member will use this classification standard as their baseline standard. If a member requires a more restrictive classification for a particular class of information due to state, federal or other agreements, the more restrictive classification will apply.
2. The A&M System Information Classification Standard will be used to assess information access and security requirements for information to be stored or processed within member shared information centers.
3. When determining security controls to use for a given set of information, Information Owners and Custodians should also assess whether special requirements exist regarding importance of information 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 Public.
4. Some classes of information may have attributes, such as "mission critical" or "business critical". Information attributes do not supplant these classifications but should be used to clarify their importance to the institution.

**State of Texas Requirement:**

State *Information Security Standards* mandate that institutions of higher education define information classification categories and establish corresponding controls. "State 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 controls for each[.]" 1 Tex. Admin. Code § 202.74(b)(1).

| | POTENTIAL IMPACT | | |
|---|---|---|---|
| **Security Objectives** | **LOW** | **MODERATE** | **HIGH** |
| ***Confidentiality***<br>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***<br>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***<br>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 on 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 on 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 on organizational operations, organizational assets, or on individuals. |

Using the table above, any particular set of information 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 information that may have low need for confidentiality, (LOW Impact) but require HIGH availability. For such information, encryption may not be appropriate, but redundancy may be a requirement. Most breaches that cause HIGH impact are a result of unauthorized access to Confidential information. Therefore, ***the A&M System's Information Classification Standard and assignment of classification places prime importance on the level of Confidentiality required of the information.***