Division of
Information Technology

Texas A&M University
Data Classification Standard

Table of Contents

Purpose

The Texas A&M University (TAMU) Data Classification Standard is intended to help data stewards, data owners, resource custodians and Information Technology (IT) personnel across the TAMU colleges, agencies, divisions and departments categorize their information and information systems, according to the impact of loss and sensitivity of data they contain. Categorization will help departments allocate their resources, prioritize the selection and placement of security controls, and ensure that systems containing sensitive information meet baseline security standards.

In classifying data, the university:

- Uses a risk-based approach to help faculty, researchers, staff, and students identify the data they use, understand its level of sensitivity, and learn how to best secure it.
- Seeks to balance protection of the confidentiality, integrity, and availability of the data needed for the TAMU academic, administrative, research, and clinical missions, recognizing the need for collaboration and sharing of knowledge across campus and the world.

Scope

The data classifications in this standard apply to all university electronic data stored, processed or transmitted on university resources or other resources where university business occurs. This includes, but is not limited to, data stored at data centers, data accessed by or stored remotely on IT Resources, or stored with agencies, contracted third parties including business associates, cloud service providers, vendors, contractors and temporary staff.

When a specific set of data is classified as fitting within a combination of two or more of the data classifications, that data shall be managed according to the most restrictive/secure applicable data classification.

Under this data classification model, data is classified in accordance with federal and state regulations, internal standards and other contractual requirements. This data classification model in no way supersedes any state or federal government classifications.

Ownership

Texas A&M University data/information is not owned by a single team, college, division, department, research team, or individual system owner, but is a university asset that is owned by Texas A&M. However, to govern and manage data appropriately, colleges, divisions and departments should identify and assign certain roles and responsibilities to staff members. These staff members play a critical role in governing Texas A&M data.

Information and information resources solely possessed by Texas state agencies must be managed as valuable state resources.

Data Sharing

The sharing and disclosure of all data owned by the university or its agencies shall follow federal and state regulation. In the absence of any federal or state regulation governing the sharing or disclosure of a particular type of data, the Texas A&M University policy or standard will be followed.

Roles and Accountability

Data Trustee

A data trustee has oversight responsibility for the portion of university data that is related to the university functions managed, administered or run by the units and personnel who report to him or her. Data trustees are institutional officers (Associate Director, Director, Associate Dean, Dean, Associate VP, C-Level, VP) who are appointed by the president or

provost and have authority over business definitions of data, and the access and usage of that data, within their delegations of authority. Each data trustee appoints data stewards for their specific subject area domains (i.e. financial, Information Technology, certain colleges or departments, etc.).

Data Steward

A data steward is responsible for the quality and integrity of a defined dataset on a day-to-day basis (from a data management perspective). Data stewards must retain responsibility for the data content, quality and integrity. They are an integral part of defining system requirements for data use and have a responsibility to protect the data from misuse or mismanagement. Data stewards promote data management and security, consider information security when budgeting and business planning, ensure accurate, valid, and timely collection of data, and ensure their data is classified according to Texas A&M data classification standard.

Data Custodian

A data custodian belongs to the Information Technology or Operations area and will manage access rights to data they oversee. Data custodians help implement adopted Division of IT controls to ensure the integrity, security and privacy of their data.

Data stewards and data custodians work closely to ensure that their college, division, or department complies with the data classification standard and any enterprise data management policies. They ensure critical data-related issues are escalated to the Texas A&M Division of IT.

Data stewards and data custodians can be the same person or team.

Data custodians perform several key data management functions, including:

- Identifying or assisting the data steward in identifying systems of record-containing institutional data
- Categorizing institutional data within systems of record according to Division of IT security and privacy guidelines
- Implement controls required to protect information and information resources
- Educating and sharing best practices with other data management personnel
- Adhere to monitoring techniques and procedures for detecting, reporting, and investigating incidents
- Ensure information is recoverable in accordance with risk management decisions.

Note:
Data trustees, data stewards and data custodians are responsible for periodic reviews to ensure the classification remains accurate, and that the application, database or system meets baseline security standards and is compliant with all federal and state regulations, and with all university standards.

Classification Levels

This section outlines four classification levels (restricted, confidential, controlled, public). Data owners, data stewards and resource custodians should ensure the selection of security controls is appropriate for the sensitivity of the data being protected. Systems that process confidential or restricted data are inherently costlier to secure and maintain. Whenever possible, avoid the unnecessary use or collection of such data.

Restricted (Extreme Impact / Sensitivity)

Restricted information is the highest level of classification and use is limited to explicitly designated individuals or groups of individuals with a stringent business need to know.

Impact of Loss
Misuse or unauthorized collection, disclosure, compromise, alteration or destruction of restricted data could result in the compromise of national security, long-term and catastrophic financial damage, and/or cause long-term and severe or catastrophic harm to Texas A&M University, its stakeholders and reputation. Restricted data also includes data that, if compromised, may lead to the bodily or physical harm of individuals.

Examples of Restricted Data

- Highly Classified Research
- Top-Secret Government Information
- Passwords to DoD or DoS workers/contractors
- Classified information relating to defense articles and defense services
- Information covered by an invention secrecy act
- Witness protection information
- Child welfare and legal information about minors (juvenile justice, foster care and/or adoption)
- Certain individually identifiable medical records and genetic information, categorized as extremely sensitive
- Research information classified as Level 5 by an IRB or otherwise required to be stored or processed in a high security environment and on a computer not connected to the Texas A&M data networks

Reporting and Discovery

- Data Stewards, Data Custodians, and Data Trustees of restricted data are responsible for identifying the systems and applications that hold restricted data.
- Data Stewards, Data Custodians, and Data Trustees of restricted data are also responsible for providing a list of assets and systems that hold restricted data in their department, division, agency, or college to Texas A&M IT security.

Infrastructure Location

- Any system, platform, software, or application that contains restricted data should be housed in a Texas A&M data center, supported by Texas A&M IT. Exceptions are evaluated on a case-by-case basis.

Security Controls

- Any system, platform, software, or application that contains restricted data should have the required Texas A&M IT security-managed controls applied.

Access

- Access shall be limited to authorized university officials or agents with a documented, verified/cleared, and legitimate need to know.
- All access to restricted data shall be monitored and logged; access logs should be available for auditing and review.
- Access logs shall be archived for any period of time required by federal or state law or for a period of 1 year, whichever is longer.
- Multi-factor authentication is required where possible.

Electronic Transmission

- Not permitted without express authorization or unless required by law.
- Secure, authenticated connections or secure protocols shall be used for transmission of restricted data. If authorized, data shall only be included in messages within an encrypted file attachment or via authorized, secure systems**.**

Storing

- On removable drives: Not permitted unless required by law. When required by law, only allowed on encrypted and password-protected devices.
- On endpoint: Systems shall comply with Texas A&M IT security requirements
- On server: (including internal cloud): Systems shall comply with Texas A&M IT security requirements and be housed in a Texas A&M data center, supported by Texas A&M IT.
- On external cloud: Not permitted without express authorization or unless required by law.

Disposal

- Data shall be deleted and unrecoverable (e.g. eraser, zero-fill, DoD multipass, etc.).
  Physical media (e.g. paper, CD, tape, etc.) should be destroyed so data on the media cannot be recovered or reconstructed.

**Corresponding Texas A&M System Classification: Confidential*

Confidential (High Impact / Sensitivity)

This classification level is reserved for information that would, if inadvertently released, have a significant or severe adverse impact to the university. This university data is protected specifically by federal or state law or Texas A&M rules and regulations. Such information may also be subject to state or federal breach notification requirements. This category also focuses on information restricted through certain legal agreements.

Use of this data is limited to authorized individuals with approved and appropriate/ required need to access, and who have signed confidentiality agreements (where applicable).

Impact of Loss

- Adverse impact on donors, consumers, employees or students.
- Moderate to significant regulatory, reputational and/or financial risk.
- Long-term loss of research funding from granting agencies.
- Increase in regulatory requirements.
- Loss of critical campus or departmental service(s).
- Loss of valuable research data or unauthorized tampering of research data.
- Potentially results in federal or state regulatory fines.
- Individuals put at risk for identity theft.

Examples of Private Data

- Federal tax information received or derived from the IRS or secondary sources
- Financial aid data
- Protected health information (HIPAA/HITECH)
- Individual financial information subject to GLBA
- Social security numbers
- Debit or credit card numbers
- Driver's license information or state identification card information
- Bank account numbers or information with personal identification numbers or passwords
- Passport numbers
- Data that falls under GDPR
- Dates of birth (if linked to other information about a person)
- Student education records that are not part of the campus directory
- Any student information under FERPA (in accordance with University rule 13.02.99.M0.01 & Texas State HB 4046)
- Electronic signatures, biometric information, password information and private encryption keys (depending on use)
- Criminal background checks
- Personally identifiable information (PII) -protected and non-sensitive
- Donor/alumni information
- Human subject information
- Sensitive digital research data
- Export controlled information – ITAR and EAR - Information or technology controlled under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)
- University financial data

Reporting and Discovery

- Data stewards, data custodians, and data trustees of confidential data are responsible for identifying the systems and applications that hold confidential data.
- Data stewards, data custodians, and data trustees of restricted data are also responsible for providing a list of assets and systems that hold confidential data in their department, division, agency, or college to Texas A&M IT security.

Infrastructure Location

- Any system, platform, software, or application that contains confidential data should be housed in a Texas A&M data center, supported by Texas A&M IT. Exceptions are evaluated on a case-by-case basis.

Security Controls

- Any system, platform, software, or application that contains confidential data should have the required Texas A&M IT security-managed controls applied.

Access

- Access shall be limited to those with a documented and business need to view or manage the data.
- All access to restricted data shall be monitored and logged; access logs should be available for auditing and review.
- Access logs shall be archived for any period of time required by federal or state law or for a period of 6 months, whichever is longer.
- Multi-factor authentication is required where possible.

Electronic Transmission

- Secure, authenticated connections or secure protocols shall be used for transmission of confidential data. If authorized, data shall only be included in messages within an encrypted file attachment or via authorized secure systems that allow for encryption.

Storing

- On removable drives: Not permitted unless documented business need and only on encrypted and password-protected devices.
- On endpoint: Systems shall comply with Texas A&M IT security requirements.
- On server (including internal cloud): Systems shall comply with Texas A&M IT security requirements and be housed in a Texas A&M data center, supported by Texas A&M IT.
- On external cloud: Not permitted without Texas A&M IT security review and assessment as well as data trustee approval.

Disposal

- Data shall be deleted and unrecoverable (e.g. eraser, zero-fill, DoD multipass, etc.).
  Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.

**Corresponding Texas A&M System Classification: Confidential*

Controlled (Moderate Impact / Sensitivity)

University data not otherwise identified as confidential or restricted, but which may or may not be releasable in accordance with the Open Records Requests or Texas Public Information Act (e.g., contents of specific email, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release (if applicable).

Protection of this data is required by the data steward or other confidentiality agreement. Access to this data is restricted to authorized individuals with approved access or a business need to access this information.

Impact of Loss

- Short-term loss of non-critical university services.
- Short-term loss of critical or non-critical departmental services.
- Unauthorized tampering of research data.
- Individuals potentially or indirectly put at risk for identity theft.
- Disclosure of data the university has chosen to keep confidential.

Examples of Controlled Data

- Non-public administrative or operational data (e.g. employee evaluations, asset listings and locations, etc.)
- Non-restricted research data
- Information used to validate identity (name plus date of birth, mother's maiden name, etc.).
- Email contents
- Employee information not listed as restricted (home address, telephone number, income tax withholdings, personal email address, race, ethnicity, marital status)
- Agency policies, procedures and/or standards
- Training materials
- Internal meeting information
- Direct telephone line numbers to staff
- Personal email addresses
- Home telephone numbers
- Employee home address information
- Emergency contact information
- Controlled unclassified data
- Unpublished research work and intellectual property not in Level 3 or 4
- Research information classified as Level 2 by an IRB
- Patent applications and work papers, drafts of research papers
- Building plans and information about the university physical plant

Reporting and Discovery

- Data stewards, data custodians, and data trustees of controlled data are responsible for identifying the systems and applications that hold controlled data.
- Data stewards, data custodians, and data trustees of controlled data are also responsible for providing a list of assets and systems that hold controlled data, in their department, division, agency, or college to Texas A&M IT security.

Infrastructure Location

- Some (based on a case-by-case evaluation) systems, platforms, software, or applications that contain controlled data should be housed in a Texas A&M data center, supported by Texas A&M IT, where possible. The determination can be made by Texas A&M IT on a case-by-case basis.

Security Controls

- Any system, platform, software, or application that contains controlled data should have the required Texas A&M IT security-managed controls applied.

Access

- Access shall be limited to authorized users only or processes acting on behalf of authorized users.
- All access to controlled data shall be monitored and logged; access logs should be available for auditing and review.
- Access logs shall be archived for any period of time required by federal or state law or for a period of 3 months, whichever is longer.
- Multi-factor authentication is required where possible.

Electronic Transmission

- Secure, authenticated connections or secure protocols shall be used for transmission of controlled data. If authorized, data shall only be included in messages within an encrypted file attachment or via authorized secure systems that allow for encryption**.**

Storing

- On removable drives: Not permitted unless documented business need and only on encrypted and password-protected devices.
- On endpoint: Systems shall comply with Texas A&M IT security requirements
- On server (including internal cloud): Systems shall comply with Texas A&M IT security requirements and be housed in a Texas A&M data center, supported by Texas A&M IT.
- On external cloud: Not permitted in most cases without Texas A&M IT security review and assessment as well as data trustee approval. Texas A&M IT should be informed to determine whether security assessment and review is needed.

Disposal

- Data shall be deleted and unrecoverable (e.g. eraser, zero-fill, DoD multipass, etc.).
  Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.

**Corresponding Texas A&M System Classification: Controlled*

Public (Low Impact / Sensitivity)

The lowest data classification level includes data openly available to the public. This might include low-sensitivity data which, when openly distributed, presents no risk to the university. This might also include official university communications and public announcements.

Systems distributing low sensitivity data can still pose a risk to the university. High-visibility public websites sharing only low sensitivity data can be targets for individuals seeking to embarrass the university and damage its reputation.

Examples of public data

- Public directory information
- Directory information about students who have not requested a FERPA block
- Faculty and staff directory information
- Research publication information
- Course catalog information
- Employee ID
- Data covered by non-disclosure agreements, service level agreements, grants, etc.
- Intercollegiate sports information (team rosters, statistics, scores, schedules)

Reporting and Discovery

- Data stewards, data custodians, and data trustees of public data are responsible for identifying and documenting the systems and applications that hold public data.

Infrastructure Location

- Some (based on a case-by-case evaluation) systems, platforms, software, or applications that contain public data and are considered enterprise-wide systems should be housed in a Texas A&M data center, supported by Texas A&M IT, where possible. This will be determined on a case-by-case basis.

Security Controls

- Any system, platform, software, or application that contains public data should have the minimum required Texas A&M IT security-managed controls applied.

Access

- Multi-factor authentication is required, where reasonable and possible.

Electronic Transmission

- As a best practice, where possible, secure, authenticated connections or secure protocols shall be used for transmission of public data.

Storing

- On removable drives: Systems shall comply with Texas A&M IT security requirements
- On endpoint: Systems shall comply with Texas A&M IT security requirements
- On server: Systems shall comply with Texas A&M IT security requirements.

Disposal

- Data shall be deleted prior to disposal

**Corresponding Texas A&M System Classification: Public*

Definitions

Extreme, High, Moderate, and Low

Security Objective	Impact			
	LOW	MODERATE	HIGH	EXTREME
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **very limited** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have an **impactful or serious adverse** effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a **serious or severe adverse** effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **very limited** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have an **impactful or serious adverse** effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious or severe adverse** effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets or individuals.
Availability Ensuring timely and reliable access to and usage of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **very limited** adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have an **impactful or serious adverse** effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious or severe adverse** effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets or individuals.

Personally Identifiable Information (PII)

PII is protected by federal and state laws and regulations, including federal regulations administered by the United States Department of Homeland Security (DHS), and is defined by DHS as "any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."

PII must be protected prior to release in accordance with federal and state disclosures required by law. PII is divided into two categories:

A. Protected

B. Non-Sensitive

PII includes but is not limited to any of the following stand-alone elements:
A. Full social security number (SSN)
B. Driver's license or state ID number
C. Passport number
D. Visa number or alien registration number
E. Fingerprints or other biometric identifiers

OR

Full name in combination with:
A. Mother's maiden name
B. Date of birth
C. Last 4 digits of SSN
D. Citizenship or immigration status
E. Ethnic or religious affiliation

Protected Health Information (PHI)

PHI is protected by the federal Health Insurance Portability and Accountability Act (HIPAA) and includes all individually identifiable information that relates to the health or health care of an individual, and specifically includes but is not limited to the following:
Any PII field in combination with the following medical modifiers:
A. Diagnosis or ICD code
B. Treatment or CPT code
C. Provider name or number
D. DEA number
E. Physician name
F. Treatment date
G. Patient notes
H. Psychiatric notes
I. Patient photos
J. Radiology images
K. MRN number

In addition, HIPAA requires the de-identification of PHI by the removal of:

- Geographic data
- All elements of dates
- Telephone numbers
- FAX numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers

- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Device identifiers and serial numbers
- Web URLs
- Internet protocol addresses
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Full face photos and comparable images
- Any unique identifying number, characteristic or code

Payment Card Industry (PCI) Data

PCI Data is data subject to the Payment Card Industry Data Security Standards (PCI-DSS), developed by the PCI Security Standards Council and adhered to by the university, and includes but is not limited to the following cardholder data:

A. Primary account number (PAN)
B. Cardholder name
C. Service code
D. Expiration date.

Sensitive authentication data:

A. Full magnetic stripe data
B. CAV2/CVC2/CVV2/CID
C. PIN/PINBlock

Export Controlled Materials

Export controlled materials is defined as any information or materials subject to United States export control regulations including, but not limited to, the Export Administration Regulations (EAR) published by the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITAR) published by the U.S. Department of State. Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export-controlled information must be controlled as sensitive information and marked accordingly.

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations and government-wide policies. These policies are for agencies on designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI, self-inspection and oversight requirements. The rule affects federal executive branch

agencies that handle CUI and all organizations (sources) that handle, possess, use, share or receive CUI—or which operate, use, or have access to federal information and information systems on behalf of an agency. CUI replaces categories such as For Official Use Only (FOUO), Sensitive but Unclassified (SBU) and Law Enforcement Sensitive (LES). All security requirements for CUI are defined in NIST Special Publication 800-171.

General Data Protection Regulation (GDPR)
The GDPR not only applies to organizations located within the EU, but also to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. It addresses the export of personal data outside the EU.

The Family Educational Rights and Privacy Act (FERPA)
FERPA is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

Enterprise System
An application, software, or integrated set of technologies that service or affect, directly or indirectly, more than one team or department. Enterprise systems may or may not house restricted, confidential or controlled data.

While Enterprise systems are usually purchased systems from external vendors, they can also be custom developed systems created to support a specific organization's needs.

Texas A&M University Division of IT & Texas A&M IT Security
The Texas A&M Division of IT is led by Dee Childs, VP/CIO. This division's responsibility includes (but is not limited to) design, implementation and support of Texas A&M's infrastructure, network, security, IT risk management, policy, platform services, messaging and collaboration, and other enterprise systems and services.

Contact and Questions

Please send all inquiries to: *ra@tamu.edu*