



Standard Administrative Procedure (SAP)

29.01.99.L1.31 Information Classification

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

This SAP establishes responsibilities and limits for system administrators and users in regards to privacy for Texas A&M International University (TAMIU) Information Resources.

TAMIU has the responsibility of safekeeping information entrusted to it. This SAP establishes a TAMIU-wide information classification scheme and acceptable controls for each class. It applies to all users and administrators of TAMIU's Information Resources. TAMIU follows the [Texas A&M University System Standard - Data Classification and Protection](#). This SAP compliments and is subordinate to the [Texas A&M University System Standard - Data Classification and Protection](#).

This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

1. Information Classification

- 1.1 **Confidential** – TAMIU data protected specifically by federal law, state law, or Texas A&M University System (TAMUS) rules and regulations (e.g., HIPAA; FERPA; U.S. Export Controlled information; Sarbanes-Oxley, Gramm-Leach-Bliley; the Texas Identity Theft Enforcement and Protection Act; Texas A&M University System Policies, etc.) TAMIU data which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non-Disclosure Agreements, etc.) TAMIU data with a statutory requirement for notification to affected parties in case of a

confidentiality breach. Examples of confidential data may include, but are not limited to, the following:

- 1.1.1 Personally Identifiable Information such as a name in combination with Social Security Number (SSN), date of birth (DOB) and/or financial account numbers.
 - 1.1.2 Banner ID in combination with Social Security Number (SSN), date of birth (DOB) and/or financial account numbers.
 - 1.1.3 Student education records protected by FERPA.
 - 1.1.4 Intellectual property as set forth in Section 51.914 of the Texas Education Code.
 - 1.1.5 Medical records (as defined by HIPAA).
 - 1.1.6 System security plans, reports, system configurations, and related information.
 - 1.1.7 TAMUS intellectual property and research information having commercial potential.
- 1.2 **Controlled** – Information that is not generally created or made available for public consumption, but may or may not be subject to release in accordance with the Texas Public Information Act (e.g., contents of specific email, financial records, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release. Examples are:
- General research information if it is classified as Controlled Unclassified Information (CUI). CUI protection, as defined by Presidential Executive Order 13556 related to the security of non-federal information systems, is applicable.
 - Staff and faculty personnel records (including Employee ID) or Banner ID
 - Licensed software/software license keys
 - Library paid subscription electronic resources
- 1.3 **Public** – TAMIU data not otherwise identified as Confidential or Sensitive. Such data have no requirement for confidentiality, integrity, or availability. Examples are:
- Public directory information
 - Public websites
 - Course listings and pre-requisites

Additional information regarding directory information can be obtained from the Office of the University Registrar at 956-326-2250.

Related Statutes, Policies, Regulations, or Rules

[Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education](#)

[Texas A&M University System Standard - Data Classification and Protection](#)

TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources

TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:

Copyright Act of 1976

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The State of Texas Information Act

Texas Government Code, Section 441

Texas Administrative Code, Chapter 202

IRM Act, 2054.075(b)

The State of Texas Penal Code, Chapters 33 and 33A

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310