STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.09 Information Resources – Privacy

Approved July 18, 2005
Revised December 4, 2009
Revised August 14, 2013
Revised July 12, 2022
Next scheduled review: July 12, 2027

Standard Administrative Procedure Statement

This SAP establishes responsibilities regarding management and protection of Personally Identifiable Information (PII) stored on university information resources.

Definitions

Chief Information Security Officer (CISO) – The TAMU CISO is responsible for developing and **implementing a comprehensive information security and IT risk management program to meet International, Federal, State and University regulations, policies, and practices. The CISO serves as the designated Information Security Officer (ISO) in accordance with TGC §2054.136 and TAC§202.71.**

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resource Owner - an entity responsible:

1) for a business function; and,
2) for determining controls and access to information resources supporting that business function.

Personal Identifiable Information (PII) – In accordance with Texas Business & Commerce Code §521.002, information that alone or in conduction with other information identifies an individual. The precise scope of information that constitutes PII may change based on context or legal jurisdiction.

Sensitive Personal Information (SPI) – PII that meets the criteria outlines in Texas Business & Commerce Code §521.002.

Privacy Officer – The TAMU Privacy Officer oversees the privacy requirements to ensure that the appropriate privacy policies have been developed and implemented and that the proper training has taken place. The Privacy Officer oversees compliance with international, federal, state, and University privacy policies, regulations, and practices. The Privacy Officer will also work on contractual matters regarding privacy to ensure compliance and to ensure that the appropriate structure has been developed to meet those specified requirements.

Applicability

This Standard Administrative Procedure applies to data that is stored, processed, or transmitted on any information resources where university business occurs.

The information resource owner, or their designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.03.M1.03 *Exceptions from Required Risk Mitigation Measures*.

The audience is all users of university information resources.

Procedures

1. The university collects and processes many different types of information from third parties. Much of this information is sensitive/PII, and shall be protected in accordance with all applicable regulations and contractual agreements (including, but not limited to: FERPA, HIPAA/HITECH, FISMA, GLBA, PCI DSS, Texas Administrative Code Chapter 202, and any other applicable state, federal, or international regulations).

2. The Chief Information Security Officer (CISO) shall implement information security to protect PII from inappropriate disclosure.

3. Individuals who have access to information because of their position have the responsibility to access and manage that data appropriately (see SAP 29.01.03.M0.02 *Information Resources - Acceptable Use*) and in accordance with any contractual or regulatory obligations.

4. Users of TAMU information resources must call Texas A&M IT Helpdesk (979-845-8300) to report any known or suspected unauthorized disclosure of PII immediately upon discovery of the incident.

Related Statutes, Policies, or Requirements

Defense Contract Management Agency Policy
Family Educational Rights and Privacy Act
Federal Information Security Modernization Act
Health Insurance Portability and Accountability Act
Health Information Technology for Economic and Clinical Health Act
NIST Special Publication 800-171 Protecting Controlled Unclassified Information
Gramm-Leach-Bliley Act
The Payment Card Industry Data Security Standard
Texas Administrative Code, Chapter 202 Information Security Standards
Texas Government Code, Chapter 2054 Information Resources
Texas A&M University System Regulation 29.01.03 Information Security
Texas A&M University System Notification Matrix
Texas A&M University Data Classification Standard
Texas A&M Information Security Controls
Texas Business and Commerce Code, chapter 521 section 002

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Vice President for Information Technology & Chief Information Officer