STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.01 Security of Electronic Information Resources

Approved May 27, 2002
Revised May 28, 2009
Revised October 15, 2013
Revised July 18, 2016
Revised October 25, 2019
Revised September 2, 2021
Next scheduled review: September 2, 2026

SAP Statement

Texas A&M University's (Texas A&M) electronic information resources are vital academic and administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the confidentiality, integrity, and availability of the University's information resources. The purpose of this Standard Administrative Procedure (SAP) is to establish the responsibilities and information security controls necessary to maintain the confidentiality, integrity, and availability of those information resources.

Definitions

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include university employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the university and/or the owner.

High Impact Information Resources - Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- result in major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Information Resources (IR) - the procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report and transmit information.

Information Security Risk Assessment Procedures (ISRAP) - Instructions and related information regarding the methodology for performing the annual information security risk assessment.

Low Impact Information Resources - Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Moderate Impact Information Resources - Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Owner of an Information Resource - a person responsible for a business function and for determining controls and access to information resources supporting that business function.

Residual Risk - The risk that remains after controls are taken into account (the net risk or risk after controls).

Security Program - The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Texas A&M Information Security Controls Catalog - a catalog of information security risk mitigation measures (controls) that represent the implementation by Texas A&M of the requirements provided by Texas Administrative Code, Title 1, §202.76 Security Control Standards Catalog.

Unit - An organizational division of Texas A&M such as an academic department or an administrative function reporting to a Department Head (academic) or Director, Executive Director, etc. (administrative).

University Data - data or information that is in the possession, or under the control, of an individual (i.e., owner, custodian, or user) by virtue of that person's employment or affiliation with the university.

Official Procedure and Responsibilities

1. GENERAL

1.1 Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the university's information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.

1.2 Appropriate data classification of information resources is a key factor to determine protection measures that are based on value and associated risks.

1.3 Texas A&M, as a State University, is required to comply with Texas Administrative Code, Title 1, Chapter 202 (TAC 202). TAC 202 assigns the ultimate responsibility for the security of information resources to the President of the University.

1.4 Texas A&M is required to comply (where applicable) with federal and contractual standards and regulations related to information security, privacy, and technology (including, but not limited to: FERPA, HIPAA, HITECH, Executive Order 13556, federal export controls, FISMA, GLBA, PCI DSS, and other applicable federal regulations).

2. RESPONSIBILITIES

2.1 The university's Chief Information Security Officer (CISO) has the explicit authority and responsibility to administer the information security requirements of TAC 202 and this SAP institution wide.

2.2 The head or director of a unit shall be responsible for ensuring that an appropriate security program is in effect and that compliance with TAC 202, federal regulations, contractual standards, and this SAP is maintained for information resources owned and operationally supported by the unit.

2.3 All university data maintained on information resources must be afforded the appropriate safeguards stated in TAC 202 and applicable University Rules, SAPs, and security controls (found in the Texas A&M Security Controls Catalog); as well as applicable federal and contractual requirements. It is the responsibility of the information resource owner, or designee, to ensure that adequate security measures are in place and that an annual risk assessment is performed.

3. MANAGING INFORMATION SECURITY RISKS

3.1 An information security risk assessment shall be performed and documented by units having ownership or custodial responsibility for electronic information resources/systems. These assessments shall be performed at least annually using the Information Security Risk Assessment Procedures (ISRAP) published by the Texas A&M Chief Information Security Officer (CISO). The Dean or Vice President for the division in which the unit resides shall formally approve the results of the information security assessment (report) and any associated unit risk management plans.

3.2 Risk assessment results, vulnerability reports, and similar information shall be documented and submitted to the CISO designee in the manner specified in the ISRAP.

3.3 Approval of information security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

3.3.1 the CISO or his/her designee(s) in coordination with the information owner for information resources identified as Low or Moderate residual risk/impact;

3.3.2 the Texas A&M President or designee for all information resources identified with a High residual risk/impact.

3.4 The CISO shall report, at least annually, to the Texas A&M Chief Information Officer (CIO) and the Texas A&M President on the adequacy and effectiveness of information security policies, procedures, controls, and compliance with TAC 202 based on the annual risk assessment and other measures.

4. UNIVERSITY INFORMATION SECURITY CONTROLS CATALOG

4.1 The implementation of information security controls found in the Texas A&M Information Security Controls Catalog is mandatory unless otherwise specified.

4.2 A department or unit may employ controls for the cost-effective security of information and information resources within or under the supervision of that department/unit that are more stringent than the controls prescribed in the Texas A&M Information Security Controls Catalog if the more stringent controls:

4.2.1 contain at least the applicable control found in the Texas A&M Information Security Controls Catalog;

4.2.2 are consistent with applicable federal law, policies and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the university.

4.3 Development and adoption of the controls found in the Texas A&M Information Security Controls Catalog is the responsibility of the CISO or designee. Prior to the adoption of new or revised controls, the CISO or designee shall:

4.3.1 solicit comments regarding the proposed new or modified control(s) from appropriate constituencies at least 30 days prior to publication of proposed controls;

4.3.2 following the review of comments, formally obtain the approval of the CIO for the new or revised control(s) which will then be published in the Texas A&M Information Security Controls Catalog with an effective date for required implementation.

4.4 Information security controls shall be created or revised with consideration toward minimizing the impact to affected university units to the extent feasible by:

4.4.1 ensuring that such controls do not require the use or procurement of specific products, including any specific hardware or software;

4.4.2 ensuring that such controls provide for flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks;

4.4.3 provide risk based required implementation dates, following the publication of the new or revised control; and

4.4.4 using flexible, performance-based controls that permit the use of off-the-shelf commercially developed information security products as appropriate.

Related Policies, Statutes, Procedures

1 Texas Administrative Code Chapter 202 *Information Security Standards*

System Regulation 29.01.03 *Information Security*

The Texas A&M University System Information Security Standards

Information Security Risk Assessment Procedures (ISRAP)

Texas A&M Security Controls Catalog

Family Educational Rights and Privacy Act

Health Insurance Portability and Accountability Act

Health Information Technology for Economic and Clinical Health Act

NIST Special Publication 800-171 Protection Controlled Unclassified Information

Federal Information Security Modernization Act

Defense Contract Management Agency Policy

The Payment Card Industry Data Security Standard

Contact Office

Office of the Chief Information Security Officer

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