STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.05 Information Resources – Enterprise Data Centers

Approved January 15, 2019
Next scheduled review: January 15, 2024

Standard Administrative Procedure Statement

To ensure Texas A&M University's moderate or high impact information resources remain available, secure, and compliant with federal, state, and other policies, such resources shall reside in a Texas A&M University Enterprise Data Center.

Definitions

Cloud Computing – has the meaning assigned by Special Publication 800-145 issued by the United States Department of Commerce National Institute of Standards and Technology: a model for enabling access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort.

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.

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 Custodian – 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.

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

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.

Significant IT Equipment (as found in System Regulation 29.01.03 §5.2) – Equipment used as part of a high or moderate impact information resource is considered "significant IT equipment". Examples include, but are not limited to:

- Mass storage. A device is considered in scope if ALL the following conditions are met:
  - Networked-accessible data storage.
  - Data has significant operational, financial, or reputational risk if lost or stolen.
  - Data can be effectively stored and accessed across existing network infrastructure without material performance or design constraints.

- Large/complex computational environments. A system or environment is considered in scope if ALL of the following conditions are met:
  - System or service provided by the system is purposefully made accessible outside of the Texas A&M network security perimeter.
  - Data has significant operational, financial, or reputational risk if lost or stolen.
  - Services provided by the system can be effectively accessed and utilized across existing network infrastructure without material performance impact.

- Most virtualized or physical-based servers. A server is in scope if ALL the following conditions are met:
  - System or service provided by the system is purposefully made accessible outside of the Texas A&M network security perimeter.
  - Data has significant operational, financial, or reputational risk if lost or stolen.
  - System can be effectively accessed and utilized across existing network infrastructure without material performance impact.

- Any other internet exposed services. An Internet service is in scope if ANY of the following conditions are met:
  - Service is purposefully made accessible outside of the Texas A&M network security perimeter.
  - Loss of the system or system's data presents significant operational, financial, or reputational risk.
  - Service and/or related systems are not receiving regular security patches from vendors and service developer(s).

Texas A&M University Enterprise Data Center – A facility used to house computer systems and associated components that is owned, managed, or contracted by the Texas A&M University Vice President for Information Technology and Chief Information Officer.

Official Procedure and Responsibilities

---

1. GENERAL

The purpose of this Standard Administrative Procedure (SAP) is to identify the types of information resources that are considered to be high or moderate impact and must reside in the University's enterprise data center.

Texas A&M University is required to comply (where applicable) with federal and state security, privacy, and information technology standards and regulations found in:

- The Federal Health Insurance Portability and Accountability Act (HIPAA),
- The Federal Health Information Technology for Economic and Clinical Health (HITECH) Act,
- The Federal Family Educational Rights and Privacy Act (FERPA),
- The Federal Information Security Management Act (FISMA),
- The Payment Card Industry Data Security Standard (PCI DSS),
- Federal Controlled Unclassified Information (CUI) Established by Executive Order 13556,
- Federal Export Controls,
- Defense Contract Management Agency (DCMA) Policies,
- Texas Health and Safety Code, Chapter 181, Medical Records Privacy,
- Texas Administrative Code, Chapter 202, Information Security Standards,
- Texas Government Code, Chapter 2054, Information Resources,
- Security and availability requirements for NSF, DoD, and DoE Research grants, and
- Other applicable federal, state, and system regulations.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all University information resources, excluding those hosted by a cloud computing provider approved by the Vice President for Information Technology and Chief Information Officer.

This SAP only applies to information resources owned by Texas A&M University.

The intended audience includes, but is not limited to, all University information resource owners and custodians.

3. PROCEDURES

3.1 All high or moderate impact information resources must:

3.1.1 Reside in a Texas A&M enterprise data center;

3.1.2 Be documented and maintained in the designated Texas A&M risk management system, including disaster recovery and backup information; and

3.1.3 Follow all applicable Texas A&M information security controls.

3.2 Terms and conditions for the use of a Texas A&M University enterprise data center are determined by the Vice President for Information Technology and Chief Information Officer.

3.3 The Vice President for Information Technology and Chief Information Officer shall maintain an "Approved List of Cloud Computing Providers" which enumerates commercial service providers that are approved for the purposes of hosting moderate or high impact information resources. A copy of such list may be obtained directly from the office of the CIO, or may be obtained electronically via the office website.

4. EXCEPTIONS

The information resource owner or designee is responsible for ensuring that the procedures 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 except certain risk mitigation measures provided in this SAP (e.g. research-related agreements that require data be hosted outside of Texas A&M University). All exceptions must be in accordance with SAP 29.01.03.M1.27 *Exceptions from Required Risk Mitigation Measures*.

Final approval for exceptions to System Regulation 29.01.03 §5.2 must come from the Texas A&M System Chancellor.

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

NIST Special Publication 800-171 Protecting Controlled Unclassified Information

The Payment Card Industry Data Security Standard

1 Texas Administrative Code Chapter 202 Information Security Standards

Texas Government Code, Chapter 2054 Information Resources

Texas A&M University Data Classification Standard

Texas A&M System Regulation *29.01.03 Information Security*

Texas A&M Information Security Control RA-2 Security Categorization

---

Contact Office

CONTACT: Office of the Chief Information Security Officer.

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