STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M0.13 Information Resources – Cloud Computing Services

Approved December 11, 2019
Next scheduled review: December 11, 2024

Standard Administrative Procedure Statement

Cloud computing services offer many advantages, such as on-demand self-service provisioning, rapid elasticity, resource pooling, and highly granular metering of resources. Along with traditional on-site information resources, Texas A&M University will consider cloud computing services to meet university needs.

However, without adequate controls, use of cloud computing services can expose Texas A&M University to costly risks. No matter where an information resource is hosted, Texas A&M University must continue to ensure that university data is properly managed, that privacy requirements are met, and that compliance with all relevant standards and regulations is verified.

Definitions

Cloud Computing – 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. Cloud computing service models include Infrastructure as a Service, Platform as a Service, and Software as a Service.

Cloud Infrastructure – A cloud infrastructure is the collection of hardware and software that enables cloud computing. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics.

High Impact Information Resource – 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 – 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.

Infrastructure as a Service (IaaS) – A model of Cloud Computing that allows a consumer of the service to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud Infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

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.

Platform as a Service (PaaS) – A model of Cloud Computing that allows a consumer of the service to deploy consumer-created applications onto Cloud Infrastructure by using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud Infrastructure—including network, servers, operating systems, or storage—but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS) – A model of cloud computing that allows a consumer of the service to use the provider's applications running on a Cloud Infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying Cloud Infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Texas A&M University Approved Cloud Computing Service Provider – A third-party vendor providing Cloud Computing services through a specific service model (IaaS, PaaS, SaaS) that has been approved by the Vice President for Information Technology and Chief Information Officer, or designee.

Official Procedure and Responsibilities

---

1. GENERAL

1.1. This Standard Administrative Procedure (SAP) establishes a process whereby faculty, staff, and students at Texas A&M University can utilize Cloud Computing services without jeopardizing university resources or causing reputational or financial harm to the university.

2. APPLICABILITY

2.1. This SAP applies to all university information resources hosted by a Cloud Computing provider. The Information Resource Owner or designee (e.g., custodian, user) is responsible for ensuring that the procedures described in this SAP are implemented.

2.2. The procedures described in this SAP will come in to effect for IaaS providers on September 1, 2019, for PaaS providers on March 1, 2020 and for SaaS providers on September 1, 2020.

2.3. The intended audience for this SAP includes, but is not limited to, all Information Resource Owners, Custodians, and users of university information resources.

3. PROCEDURES

3.1. Owners or Custodians of High and Moderate Impact Information Resources hosted in Cloud Computing services must ensure that the Information Resource:

3.1.1. Is approved for use within the specific Cloud Computing provider and service model by the Vice President for Information Technology and Chief Information Officer (CIO), or designee;

3.1.2. Has a clearly designated Information Resource Owner;

3.1.3. Follows all applicable Texas A&M University Rules, SAPs, and information security controls; and

3.1.4. Abides by the Texas A&M University System Records Retention Schedule and Notification Matrix.

3.1.5. Complies (where applicable) with federal and contractual standards and regulations related to information security, privacy, and technology.

3.2. High and Moderate Impact Information Resources that are built on IaaS or PaaS services are subject to security review and approval by the Division of IT security team.

3.2.1. The Division of Information Technology shall provide a set of IaaS and PaaS services through master contracts that are managed by the Division of IT. These contracts will be compliant with all requirements of this SAP, and will provide a baseline compliance guarantee for Texas A&M information security controls.

3.3. Personal Cloud Computing services accounts (Cloud Computing services for which the service agreement is with an individual rather than the institution) may not be used to store, process, share, or manage university data classified as restricted or confidential according to the Texas A&M Data Classification Standard.

3.4. The CIO 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 this list may be obtained directly from the office of the CIO, and is available electronically on the Division of IT website.

3.4.1. Approval for Cloud Computing service providers will be granted for specific commercial service offerings and/or products for use within a specific Cloud Computing model (IaaS, PaaS, or SaaS).

3.4.2. Cloud Computing products that are authorized under the Federal Risk and Authorization Management Program (FedRAMP) will be approved with no additional requirements.

3.4.3. Cloud Computing products that do not have FedRAMP authorization can submit a Higher Education Cloud Vendor Assessment Tool (HECVAT) assessment completed by the vendor. Scores that exceed a minimum threshold determined by the Chief Information Security Officer (CISO) will be approved with no additional requirements.

3.4.4. Cloud Computing service providers that cannot meet the requirements described in 3.4.2 or 3.4.3 will be subject to a security review by the Division of IT security team prior to approval.

3.5. Cloud computing service provider contracts or service agreements shall include appropriate language from the Texas A&M Contract Administration library to enforce these procedures.

3.5.1. Texas A&M Contracts Administration will periodically review the language in the contract library in coordination with the offices of the Chief Information Security Officer and the Privacy Officer to ensure compliance with this SAP, and other applicable information security controls or privacy regulations.

4. EXCEPTIONS

4.1. 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. All exceptions must be in accordance with SAP 29.01.03.M0.03 *Exceptions from Required Risk Mitigation Measures*.

Related Statutes, Policies, or Requirements

NIST Special Publication 800-145 Definition of Cloud Computing

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

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 Information Security Standards

Texas A&M University System Notification Matrix

Texas A&M University Data Classification Standard

Texas A&M Information Security Controls

Texas A&M University SAP 25.07.01.M1.01 *President's Delegation of Authority for Contract Administration*

Contact Office

CONTACT: Office of the Chief Information Security Office

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