Standard for Cloud Services

Objective

The National Institute of Standards and Technology (NIST) defines cloud services as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The use of Cloud Services requires additional consideration and risk management to ensure the confidentiality, integrity, and availability of University Data. This document provides a set of requirements and best practices applicable to Cloud Services to ensure that University expectations for data security are achieved.

Scope

This standard applies to all Cloud Services that follow a "shared responsibility model" (see Appendix A for AWS and Appendix B for Microsoft Azure) used by UTD. This includes, but is not limited to, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Data as a Service (DaaS), or other such services where UTD manages the software or operating system. These are hereafter and collectively known as Cloud Services.

This standard does not apply to Software as a Service (SaaS) applications where the vendor fully manages the software and UTD is only a consumer of the service.

Cloud Platform Service Standards

1. **Cloud Service Procurement Standards**
   - 1.1 Each Cloud Service must have an Institution Owner. The Institution Owner can be a Department Head, Researcher, or Technical Support lead who identified a Cloud Service and considers it essential to supporting University operations. It is the Institution Owner's responsibility to:
     - 1.1.1 Obtain approval and support from their respective Department Head to acquire and use the Cloud Service. All risks and responsibility for the Cloud Service are assumed by the Institution Owner and approved by

respective Department Head.

1.1.2 Monitor and ensure the ongoing use of the Cloud Service conforms to State, UT System, and UT Dallas policies and regulations.

1.1.3 Classify the data stored or processed within the Cloud Service; assign mission criticality of the Cloud Service.

1.1.4 Ensure that a Custodian has been assigned to implement, maintain, and monitor the information security of the Cloud Service.

1.1.5 Ensure that access control and related procedures are reviewed on an ongoing basis and when access to the Cloud Service is added or removed from users.

1.2 Vendor due diligence must be performed prior to entering into an agreement with a Cloud Service provider in all cases where a network connection to internal campus resources will be established and all cases where Confidential or Controlled Data will be processed or stored within the Cloud Service. Due diligence includes more than verification of functionality and compatibility, often including regulatory compliance, information security controls, financial viability of the provider, and thorough contract negotiation. This includes ensuring that:

1.2.1 Cloud Services must be purchased and approved by the Procurement Management department, within the Office of Budget and Finance division. Purchases by OneCard or personal funds are forbidden and may not be reimbursed. For existing Cloud Services relationships, such as Amazon Web Services or Microsoft Azure, it is recommended that faculty, staff, and students leverage contracts already negotiated and established by the Office of Information Technology.

1.2.2 The terms and conditions of the Cloud Service contract must be approved by the Office of Contract Administration department, within the Office of Budget and Finance division. The “click-through” agreements on many cloud services do not meet State, UT System, and UT Dallas procurement requirements. In addition, FERPA and/or HIPAA Business Associate Agreements (BAAs) must be in place where applicable.

1.2.3 A vendor information security risk assessment must be completed. The Information Security Office (ISO) conducts risk assessments that may include using the following tools or documents:

- The Higher Education Community Vendor Assessment Tool (HECVAT) Lite Weight Version
- SOC 2 or independent information security audit report
- Manual testing using a host or web vulnerability scanner
- Additional documentation review, as necessary

1.2.4 Data within the Cloud Service can be readily accessed by the Institutional Owner or their department as the need arises or if a individual with responsibilities for the Cloud Service is no longer available in that job role.

2. Cloud Service Configuration Standards

2.1 Remote access to a desktop or terminal environment must only be achieved through an encrypted service approved by the ISO. For example, Microsoft Remote Desktop is permissible, while freeware such as RealVNC downloaded from the Internet is considered unsafe. SSH is permissible, whereas telnet is considered unsafe because it is natively unencrypted clear text.

2.2 System and application security logs should be sent to a centralized log aggregation tool, where possible. ISO may need to obtain access to logs which are not stored within the UT Dallas enterprise Splunk log aggregator.

2.3 All PaaS instances must be configured to enable software-based firewall functionality, and all relevant application, security, and system log data must be sent to the UT Dallas enterprise Splunk log aggregator.

2.4 If data is stored within a PaaS instance, backups are recommended as frequently as necessary to maintain ongoing operations, as determined by the Instututional Owner and Custodian.

2.5 Public-cloud storage for Confidential Data must be managed by Office of Information Technology or teams within the UT Dallas Federated IT model.

2.6 Cloud workloads must also meet any other applicable standards, depending on service type:

2.6.1 PaaS instances that are virtual machines providing shared resources via the Cloud Service and are best described as servers or desktops must also follow the appropriate standards published by the ISO, for example, the Standard for Servers.

2.6.2 IaaS that is developed offsite and has a risk profile similar to local infrastructure must also follow the appropriate standards published by the ISO, for example, the Network Firewall Standard.

2.6.3 SaaS or PaaS instances used to store or process Confidential Data may require additional security protection beyond this standard.

Appendix

Appendix A:

AWS Shared Responsibility Model - https://aws.amazon.com/compliance/shared-responsibility-model/

Appendix B:

Microsoft Azure: Shared Responsibility Model - https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

Revisions

Date:	**Name:**	**Changes / Notes:**
March 20, 2020	Nate Howe	Completed draft review and published as final