Cloud and Third Party Services

Original Implementation: January 26, 2016
Last Revision: None

This policy establishes the conditions and security requirements for the use of information technology vendors, third parties and cloud services providers. Third parties and cloud service providers play an important role supporting the management of technology (e.g., hardware and software) for university constituents. Stephen F. Austin State University (SFA) contracts with numerous third party vendors to provide essential services while maintaining a high level of security. Setting standards for security and access controls reduces the risk of liability, loss of revenue, loss of data, or loss of trust to the university. This policy is consistent with the requirements of Texas Administrative Code, Chapter 202 and the Security Control Standards Catalog established by the Texas Department of Information Resources.

Scope:

This policy applies to all university personnel and university confidential and/or sensitive electronic data.

Policy:

1. All SFA confidential and/or sensitive electronic data must be stored on university provided equipment (e.g., computers or servers purchased by SFA), university contracted cloud service providers (e.g., Office 365).
2. Employees will not store any SFA electronic data on personal cloud services accounts such as Dropbox, Google Docs, etc.
3. SFA has the authority to monitor information resources to ensure compliance with this policy.

Exclusions:

Faculty members, researchers and other employees working collaboratively with others outside of the university may be excluded from these requirements if the information being shared is stored in a secure manner. Additionally, data may be stored or shared through methods established by university oversight agencies such as The Higher Education Coordinating Board, State Comptroller's Office, State Auditor's Office, etc.

Definitions:

Cloud Computing – 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. Cloud computing service models include the following: Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (NIST 800-145 September 2011).

Infrastructure as a Service (IaaS) – The capability provided to the consumer is to provide 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) (NIST 800-145 September 2011).

Platform as a Service (PaaS) – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created 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 (NIST 800-145 September 2011).

Software as a Service (SaaS) – The capability provided to the consumer is 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 (NIST 800-145 September 2011).

Cross Reference: Purchase of Automated Information Systems; Tex. Gov't Code § 2157.007; Tex. Admin. Code §§ 202.1-.2, .70-.76; National Institute of Standards and Technology, Special Publication 800-145; Texas Department of Information Resources Security Controls Catalog.

Responsible for Implementation: Provost and Vice President for Academic Affairs

Contact for Revision: Chief Information Officer

Forms: None