# Cloud Based Computing Policy

## Overview

Cloud technology encompasses almost all information system infrastructures and application deployments. The current market is trending away from on-premise hardware in lieu of the increased scalability, reliability, and functionality of cloud based offerings. With this enhanced functionality comes increased responsibility to manage data security, access, and relationships between the provider and the [LEP].

Examples of common cloud service providers in the educational computing space include:

* Infrastructure providers like Amazon Web Services and Microsoft Azure
* Platform and Architectural Delivery Services like Salesforce and Google Apps
* Electronic Mail Systems like Outlook 365 and Gmail
* Learning, Administrative, and Student Management Systems like Schoology and Infinite Campus
* Utility and Shared Storage Services like Carbonite and Syncplicity

[LEP] uses cloud service providers to lower costs, increase functionality and availability, focus services, and improve customer satisfaction. Effective management and administration of third party cloud providers is critical to normal operations.

## Purpose

Cloud services provide convenient and on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services). The purpose of this policy is to establish processes and procedures for cloud service providers, their responsibilities, and management strategies to protect [LEP] applications and data.

## Scope

This policy applies to all [LEP] staff, users, and contractors that create, deploy, or support infrastructure, applications, and/or systems software in a third party hosted cloud based infrastructure.

## Policy

Cloud technology has expanded and allows almost any IT related resource to be offered as a service. Taking advantage of these benefits requires that appropriate controls and risks are managed related to the [LEP]’s assets, data, and property. The following processes and policies shall be followed when entering into cloud-based services offerings:

### [LEP] RESPONSIBILITIES

The [Insert Appropriate Role], in coordination with the [Insert Appropriate Role], shall ensure that all cloud service offerings use a consistent and repeatable process for evaluation and selection. The following procedures and processes shall, at a minimum, be followed:

**Risk Assessment** – An internal risk assessment and analysis shall be performed on all services to be housed by cloud providers. The analysis shall identify any risks to the business unit, organization, process, security, and/or data stored. As part of this work, mitigation strategies shall be prepared that identify remedies and corrective controls to address concerns.

**Procurement** **and Contract** – The [Insert Appropriate Role] or their designee shall ensure all standard [LEP] procurement policies and practices are in effect and followed regarding general procurement. The standard [LEP] contract template shall be used as the basis for all service provider relationships. All specialized terms related to student data privacy, cloud based computing, and third party providers shall be enforced. This includes but is not limited to:

* Due diligence activities including personnel background checks, length of time in business, insurance compliance and experience with similar engagements.
* Assurance that vendor personnel do not violate [LEP] policies, procedures, agreements, or related documents. [LEP] [Insert Appropriate Department] shall provide a primary point of contact for the vendor responsible for managing the relationship, Service Level Agreement (SLA), and ensuring the vendor is compliance with all contract terms.
* Periodic review of authorized cloud service providers’ personnel working on the contract and the services performed by each. These records shall be available on-demand by the vendor.
* [LEP] management shall maintain copies of all agreements and required documentation for each cloud provider engagement.
* All contracts with cloud service providers shall specify:
	+ Explicit language related to relevant security requirements including controls over the processing, accessing, communicating, hosting, and management of [LEP] data. This includes encryption, access controls, leakage prevention, and integrity controls for data exchanged to prevent improper disclosure, use, alteration or destruction of data.
	+ Confidentiality and privacy clauses protecting student and employee data.
	+ Physical and role based security access to [LEP] data and applications.
	+ Data security and protection methods used by the service provider.
	+ Acceptable methods for the return, destruction, or disposal of [LEP] information stored on vendor resources at the end of the agreement.
	+ Acknowledgement that the service provider must only use [LEP] data for the explicit purposes defined in contract.
	+ Agreement that any information acquired by the service provider during the course of the contract cannot be used for any other purpose than that specified in the contract or divulged to others without formal written exception/condition agreed to by data owner, [LEP] and the vendor.

### CLOUD SERVICE PROVIDER REQUIREMENTS

The [Insert Appropriate Role] or their designee shall ensure each service provider complies with the following processes and procedures:

**Access to PII** - Vendor staff with access to confidential, student personally identifiable, or sensitive data must be cleared to handle that information. Access to information shall be activated only when required and needed. Access shall be deactivated after services have been provided.

**Security Incident Reporting** – Vendor must report any security incidents related to physical or logical data compromises immediately to appropriate [LEP] personnel and take all appropriate actions to mitigate the security risk.

**Termination of Service** – Vendor shall ensure that all [LEP] data is collected and returned to the [LEP] or provide written certification of data destruction within a twenty-four (24) hour window.

**Agency Requested Audits** – Vendors are required to comply with all [LEP] auditing requirements.

**Data Breaches** – Vendors shall notify [LEP] within twenty-four (24) hours upon the discovery of a service provider security breach. Upon such notification, [LEP] shall have the right, but not the obligation, to terminate the agreement with the cloud service provider. The vendors shall pay for all costs incurred to remedy the breach for [LEP], its customers, and related expenses related to the incident.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal operating processes. Examples of control and management documentation include:

* Compliant historical and current procurement documents (RFP, executed contracts, and statements of work) for current cloud provider vendors
* Internal process and archival documentation related to risk assessments and mitigation components

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/16/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |