Cloud Computing Policy

Policy Title:
Cloud Computing Policy

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy applies to all persons accessing and using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by Loyola University Chicago, all consultants or agents of Loyola University Chicago and any parties who are contractually bound to handle data produced by Loyola, and in accordance with university contractual agreements and obligations.

This policy ensures that Loyola Protected or Loyola Sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, Loyola University Chicago for services such as, but not limited to, social networking applications (i.e. all social media, blogs and wikis), file storage (See Listing of Cloud Storage Services in Appendix), and content hosting (publishers text book add-ons). Acceptable and unacceptable cloud storage services are listed in the appendix. All other cloud services are approved on a case-by-case basis.

This policy endorses the use of cloud services for file storing and sharing 1) with vendors who can provide appropriate levels of protection and recovery for university information, and 2) with explicit restrictions on storage of University Protected Information. While cloud storage of files can expedite collaboration, and sharing of information anytime, anywhere, and with anyone, there are some guidelines that should be in place for the kind and type of university information that is appropriate for

storing and sharing using these services. Even with personal use, one should be aware of the level of protection available for your data using such a cloud service.

Federal and State laws and regulations place a premium on institutions' ability to understand the risks of IT services and systems and make appropriate determinations about risk tolerance. Some cloud providers, for instance, might mine data for marketing purposes. Covered laws and regulations are listed in the Loyola University Data Classification Policy.

There are several information security and data privacy concerns about use of cloud computing services at the University. They include:

- University no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws Loss of privacy of data, potentially due to aggregation with data from other cloud consumers.
- University dependency on a third party for critical infrastructure and data handling processes
- Potential security and technological defects in the infrastructure provided by a cloud vendor.
- University has limited-service level agreements for a vendor's services and the third parties that a cloud vendor might contract with
- University is reliant on vendor's services for the security of some academic and administrative computing infrastructure.

II. Definitions

Loyola Protected Data: Any data that contains personally identifiable information concerning any individual and is regulated by local, state, or Federal privacy regulations.

Loyola Sensitive Data: Any data that is not classified as Loyola Protected Data, but which is information that Loyola would not distribute to the general public.

Loyola Public Data: Any data that Loyola is comfortable distributing to the general public.

III. Policy

The following table outlines the data classification and proper handling of Loyola data.

Data Classification	Cloud Storage (See appendix for approved services)	Network Drive *(LUC ID and Password Required)*	Local Storage
Loyola Protected	**Allowed** Provided appropriate account controls are in place (MFA).	**Allowed** No special requirements, subject to any applicable laws	**Not Allowed**
Loyola Sensitive	**Allowed but Not Advised** Requires Dept. Manager approval	**Allowed** No special requirements, subject to any applicable laws	**Allowed but Not Advised** Requires Dept. Manager approval
Loyola Public	**Allowed** No special requirements	**Allowed** No special requirements	**Allowed** No special requirements

Use of central and departmental servers, where UVID authentication is required, is the best place to store all categories of Loyola data, particularly Loyola Protected data. Loyola Protected Data can be stored on the Loyola University Chicago instance of OneDrive provided access to the data is protected by Multi-Factor Authentication and sharing is set for "People in Loyola University Chicago with the link". It is never acceptable to store Loyola Protected data on any other cloud service. This includes data such as grades, social security numbers, private correspondence, classified research, etc.

General Data Protection Terms

The University must specify data protection terms in a contract with a cloud-computing vendor. In this way, the University creates a minimum level of security for University data. A minimum level of security ensures that the University data is kept confidential, is not changed inappropriately, and is available to the University as needed.

The University should consider the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

Compliance with Legal and Regulatory Requirements

The University has many federal laws that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA).

State laws may also affect a relationship with a cloud-computing vendor. For instance, the Illinois Personal Information Protection Act (IPIPA) requires that the University must follow rules about disclosing Social Security Numbers as well as specific security breach notification procedures.

NOTE: A relationship with a cloud-computing vendor may also be impacted by private industry regulations. For example, departments at the University that accept credit cards also must follow the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the major credit card companies. Finally, cloud-computing services that use, store, or process University data must also follow applicable University policies. Such policies may include Information Technology Services policies and the University's data handling requirements.

Exit Strategy

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The University must determine how data would be recovered from the vendor.

Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

Listing of Cloud Storage Services

This listing is meant to serve only as a partial list of cloud storage services. Any cloud storage service not explicitly listed as approved should be assumed to be not approved.

Services Approved for University Use	Services Not Approved for University Use
Microsoft OneDrive (Loyola Enterprise Account using UVID and Multi-Factor Authentication only)	Dropbox
	iCloud
	Microsoft OneDrive (Personal Account)
	Amazon Cloud Drive
	Google Drive
	Box

Individuals who use enterprise OneDrive accounts for university work are responsible for ensuring that Loyola Sensitive information is not placed or stored in unapproved or

inappropriate locations. When using OneDrive for institutional information, use it only for institutional information classified as Loyola Public or Loyola Sensitive. Pay special attention to access levels when sharing files and folders with other collaborators to ensure that data is not inappropriately shared. You should not use your enterprise OneDrive account to collect, process, or store data covered by laws such as HIPAA, FERPA, FISMA, IPIPA, and GLBA. This does not include limited research datasets or fully de-identified information as related to the HIPAA Privacy Rule.

Contractual Expectations

The University will seek and endorse vendors who deliver solutions that meet the following requirements.

Both the University and cloud-computing vendor must declare the type of data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the data owned by each party. The parties also must clearly define data that must be protected.

The contract must specifically state what data the University owns. It must also classify the type of data shared in the contract according to the University's classification schema: Public, Sensitive, or Protected. Departments must exercise caution when sharing University-classified sensitive or protected data within a cloud computing service.

The contract must specify how the cloud-computing vendor can use University data. Vendors cannot use University data in any way that violates the law or University policies. Any contractual agreement for cloud services should specify that the datastore must be in onshore locations that are within the boundaries of the United States.

Cloud services utilized by individuals in the European Union must comply with the EU General Data Protection Regulation. Additionally, there may be regulatory requirements imposed by other foreign countries.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- Ownership and Use of Data
- Data Classification Policy
- Electronic Security of Loyola Protected & Sensitive Data Policy

Approval Authority:	ITESC	**Approval Date:**	August 31, 2012
Review Authority:	Jim Pardonek	**Review Date:**	July 17, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu