Cloud Computing Policy

Policy Title:

Contact(s):

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.dnla (l)10a (l (a)-1 (9e 4 s10(p
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

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

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 af

V. Roles and Responsibilities

VI. Related Policies

-
-
-
-

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