Data Protection Policy 9.1.1.G - University Approved Cloud Storage

Effective Date: 5/30/2014
Prior Effective Date: 7/1/2009

Background
The University of Cincinnati is committed in its responsibility to maintain the privacy and security of confidential personal information as well as other restricted and controlled data the university collects and preserves. While fulfilling that responsibility the university recognizes the need for a cloud storage solution that empowers and encourages faculty, staff and students to utilize a one-source secure and reliable collaborative tool that provides anytime, anywhere access to non-restricted university data. As cloud storage becomes increasingly prevalent and storage locations proliferate, the advantages of a university approved singular cloud storage provider to assist in collaborative academic and controlled research endeavors become evident. The university therefore provides a university approved cloud storage solution authorizing a secure data storage location. By providing a secure and accessible data storage solution for faculty, staff and students the university continues to promote and provide for the security of university data while maintaining data accessibility.

Data Classification Restrictions
In order to meet current data security requirements, certain restrictions need to be placed on collecting, processing, storing or sharing certain data within the cloud environment.

There are a number of Federal laws and regulations that require protection of different types of data, therefore, the Data Protection Policy was created to help provide simplified guidance and direction for compliance in a complex environment. The Data Protection Policy includes the Data Classification and Data Types appendix which explains what information must be protected, how it should be classified (Restricted, Controlled or Public), what protections are required and which laws or regulations apply.

Data that carries a university Public or Controlled classification may be stored in the university approved cloud storage location.

University data with a Restricted classification shall not be stored on any cloud storage location with the exception of Family Educational Rights and Privacy Act (FERPA) regulated data. FERPA regulated data requires a Risk Acceptance Form to be completed, approved and on file with the university and consequently is permitted to be stored in the cloud.
Data that falls under the Protected Health Information (PHI-HIPAA) classification shall not be stored in a cloud environment. In addition, any data that contains Social Security Number information shall not be stored in a cloud environment.

Data stored on the university approved cloud storage location is subject to any university eDiscovery policies.

As a result of the restrictions placed on cloud storage, faculty, staff or student members will assume responsibility and be held liable for any data breach that results from utilizing a non-university approved cloud storage provider for their university related Restricted data storage needs.
Related Links
The Data Protection Policy and all its subparts:
- Minimum Safeguards
- Data Classification and Data Types
- Roles and Responsibilities
- Acceptance of Risk Policy and Risk Acceptance Form
- Compliance and Remediation
- Summary of Applicable Laws
(More detail on the applicable laws available on the IT@UC Office of Information Security website.)
- University Approved Cloud Storage (This Document)

Contact Information
IT@UC Office of Information Security  513-558-ISEC (4732)  infosec@uc.edu

History
Issued: 7/1/2009
Revised: 5/30/2014