

Data Governance & Classification Policy 9.1.1.E - Cloud Based File Storage

Background

The University of Cincinnati is committed to maintaining the privacy and security of Controlled Unclassified Information (CUI), Restricted, and Controlled data. While fulfilling that responsibility, the university recognizes the need for a cloud-based file storage solution that empowers and encourages faculty, staff and students to utilize a secure and reliable collaborative tool that provides anytime, anywhere access to certain university data. As cloud-based file storage becomes increasingly prevalent and storage locations proliferate, the advantages of a university approved singular cloud-based file storage provider to assist in collaborative academic and research endeavors become evident. The university provides an approved cloud-based file storage solution for secure data storage. 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.

All users must use only university approved cloud-based file storage options for Restricted and Controlled data. [Box at UC](#) was previously the university's only approved cloud-based file storage option. Effective July 1, 2019, [OneDrive](#) has been approved as the new university supported online cloud-based file storage option. Box at UC will remain an approved option until further notice (likely June 30, 2020).

Controlled Unclassified Information, which includes Export Controlled data, is not permitted to be stored in any cloud storage solution, please contact the [Export Controls Office](#) and the Office of Information Security for appropriate university file storage locations.

Restricted and Controlled data is permitted to be stored on OneDrive or Box at UC. Restricted data is not permitted to sync to non-university owned devices. Sharing of Restricted data via OneDrive or Box at UC is on a need-to-know basis within the university. Any sharing outside the university must be approved by the appropriate Data Trustee or Data Steward.

The university may contract with a third-party vendor for a specific cloud-based solution. The vendor's solution must be assessed by IT@UC for compliance with appropriate safeguards and proper alignment with university Information Technology infrastructure. The [University of Cincinnati Data Security Rider](#) must be added to all vendor contracts that utilize cloud-based file storage of Restricted or Controlled university data and/or when a vendor is provided access to a university system that contains Restricted or Controlled data.

Data stored on the university approved cloud-based file storage is subject to all university eDiscovery policies and procedures.

Cloud based file storage services not purchased by the university including freely available options may not meet the universities requirements for security, privacy and records retention. As a result of the restrictions placed on cloud-based file storage, faculty, staff or students will assume responsibility and be held personally liable for any data breach, policy or legal violation that results from utilizing a cloud-based file storage provider not approved by the University.

Exit Strategy

Cloud services must 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 and/or transferred to a different vendor. The university must also work with the vendor to establish procedures on data sanitization from the vendor's cloud services.

Related Links

[Data Governance & Classification Policy](#)

Contact Information

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

History

Issued: 09/01/2009

Revised: 05/30/2014

Revised: 01/25/2017

Revised: 10/25/2017
Revised: 09/26/2018
Revised: 07/01/2019
Reviewed: 09/25/2019
Revised: 09/03/2021