Cloud Storage for the University of Baltimore
Acceptable Use and Data Security Guideline

Overview

The University of Baltimore ("University") and 3rd party vendors must negotiate contractual terms and conditions that protect the privacy and confidentiality and ensure the integrity and availability of University student, faculty, staff, and alumni data stored and used in the cloud. The paragraph and table below summarize the acceptable use and data security requirements for the specific data elements listed and for the two responsible parties involved (i.e., 3rd party vendor and the University).

Data Storage in the Cloud

Commercial cloud collaboration and storage solutions that allow users to move data such as files and folders from their computers to the Internet to be shared and easily accessed from other devices are becoming more prevalent among computer users today. Data, however, must be protected when it is not meant for public dissemination. Data moved to a commercial cloud storage solution leaves the safe confines of the University the moment you upload it and therefore can no longer be secured using University resources. Nonpublic data, which includes Personally Identifiable Information ("PII"), must therefore be handled and stored only with providers for which the University has reviewed and accepted terms and conditions. Table 1 below shows a sampling of nonpublic data elements and their corresponding cloud storage requirements. Note that only the approved cloud storage solutions listed (i.e., Microsoft OneDrive and Google Drive) may be used for cloud storage of University data. Per Table 1, nonpublic University data that is highly sensitive is not permitted in cloud storage. Note that non-PII student data protected by the Family Educational Rights and Privacy Act (FERPA) is permitted in cloud storage where indicated, provided that the information is shared only between the student and those who have a legitimate education-related interest as defined by the University's Student Records policy. FERPA protected student data, however, should never be made publicly accessible.

Table 1: Nonpublic Data Elements for Cloud Storage

Data Elements	**Regulation Source**	**Permitted for Cloud Storage?**	
		Microsoft OneDrive	Google Drive
Institution-Specific Data	University	Y	Y
Student Educational Records	FERPA	Y	Y
Personally Identifiable Information (PII)	USM/University	N	N
Protected Health Information (PHI)	HIPAA	N	N