XAVIER UNIVERSITY
Cloud Storage

Effective: May 2022
Last Updated Date: May 2022
Last Reviewed Date: May 2022
Responsible University Office: Information Technologies
Responsible Executive: Associate Vice President and Chief Information Officer

Scope: Faculty and Staff

A. REASON FOR POLICY

Xavier University is committed to maintaining the privacy and security of Export Controlled, Confidential, and Internal Use 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. 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.

B. POLICY

All Users must use only university approved cloud-based file storage options for Confidential and Internal Use data. Microsoft OneDrive and Microsoft SharePoint have been approved as the University supported online cloud-based file storage options.

Export Controlled data is not permitted to be stored in any cloud storage solution; please contact Information Technologies for appropriate University file storage locations.

Confidential and Internal Use data is permitted to be stored on OneDrive or SharePoint. Confidential data is not permitted to synchronize to non-university-owned devices.

Sharing of Confidential and Internal Use data via OneDrive or SharePoint 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.

Cloud based file storage services that are not approved by the university including freely available options may not meet the university's 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.

C. DEFINITIONS (if applicable)

Data Trustees: Data Trustees are senior university officials who have planning and policy level responsibility for defined segments of institutional data. Data Trustees assign Data Stewards, oversee the establishment of data policies, determine legal and regulatory requirements for data, and promote data quality and appropriate use of data.

Data Stewards: Data Stewards have operational planning and policy level responsibility for data within their functional areas. They assign individuals to serve as a Data Custodian from their area. In coordination with Data Custodians, they implement and apply safeguards that meet or exceed the minimum safeguards of each data classification.

Public: Public information is defined as information that is generally available to anyone within or outside of the University. Access to this information is unrestricted and may be shared internally or externally without prior approval. Public information includes, but is not limited to, marketing materials, public web site contents, University statistics or any other information that has been approved by management for public release.

Data Custodians: A Data Custodian is the individual authorized by the appropriate Data Steward to be responsible for management of data which includes maintaining and controlling data quality as well as granting inquiry, entry and updating data privileges within their respective area of responsibility. Data Custodians must be and serve as the departmental data liaison for their specific area.

Data Custodians are responsible for the accuracy and completeness of data and responsible for the maintenance and control of data validation and rules tables. These tables, and processes related to their use, define how business is conducted at Xavier University. The Data Custodians are responsible for access control data within his/her charge. They make data available to others for the use and support of the office or department's functions.

Internal use: Internal use information is defined as University information that is to be used within Xavier. Access to this data may be limited to specific departments and cannot be distributed outside of Xavier. Internal use information is less sensitive than Confidential information, but if exposed could have an adverse impact to the University.

Internal use information includes but is not limited to strategic plans or other non-public information as dictated by the Data Custodian. All information not otherwise classified will be assumed to be internal use. Users may not disclose internal use information to anyone who is not an authorized user without prior consent of the Data Custodian.

Confidential: Confidential information is defined as personal or University information that may be considered potentially damaging if released and is only accessible to authorized users. Confidential information includes, but is not limited to, medical/health information, legally privileged information, contractual information, payment card information, personally identifiable information, protected health information and protected student information. Users may only share confidential information with people that require the information to perform their job. Sensitive HIPAA and FERPA information are considered confidential and should only be shared on an as needed basis and in compliance with any applicable laws.

Export Controlled: As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology. This data is labeled Export Controlled. Users of Export Controlled data must follow all the safeguards for Restricted data plus additional safeguards as directed by The Data Trustees, Stewards, and Custodians of systems and applications that have Export Controlled data. The Custodians are responsible to identify appropriate additional safeguards.

D. PROCEDURES

Exceptions to this policy will be handled on a case-by-case basis. To attain an exception, contact the Help Desk at one of the following:

Phone: (513) 745-HELP (4357)
Link: https://services.xavier.edu/TDClient/Home/

E. EXHIBITS (if applicable)

F. HISTORY

Other applicable policies and/or resources:

Information Technology Policies

- Acceptable Use Policy
- Data Classification Policy
- IT Acquisition Policy
- Remote Access Policy