University Data Storage Standard

November 2024

Purpose:

The purpose of this standard is to outline the supported storage options available to JMU faculty, staff, and students based on the various types of University Data. This standard supports and is in accordance with University Policy 1205 – Data Stewardship.

Definitions:

Highly Confidential Data: University Data which, because of its associated legal restrictions or potential security ramifications, is approved for use only on a very limited basis and only with special security precautions. See Highly Confidential Data List.

Protected Data: University Data individually requested and approved by a Data Manager for a specific business use and subject to the general provisions associated with university information security. This includes, but is not limited to, Personally Identifiable Information (other than PII classified as highly confidential) worthy of protection and discretion in its distribution and use.

Public Data: University Data that can be shared without restriction with the general public.

University Data: Data collected, maintained or used by university personnel, contractors, or partners as part of their job responsibilities, for operation of the University, or to fulfill its mission. University Data may reside in different automated systems and in different physical locations, but are to be considered part of a single, shared resource. This resource consists of information represented in a variety of data elements, types, and forms maintained by individuals, administrative/academic units or business partners to provide functionality to the University. All such data owned and managed by or on behalf of the University are considered University Data unless explicitly noted otherwise in writing.

Standard:

1. Storage Options

The University provides multiple options for document storage; however, not all options are appropriate for every type of University Data. The following chart outlines JMU storage options and the approved University Data for each option. When evaluating storage options, users should consider the type of data being handled/stored as well as collaboration and sharing requirements.

In addition, users handling/storing Highly Confidential or Protected Data must use Microsoft Sensitivity Labeling for further protection. For more information on Sensitivity Labeling, see Microsoft 365 at JMU.

		Protected Data			High Confidential (HC) Data			
	Public Data	FERPA	PII	Other Protected	GLBA	Health	Research*	General HC
JMU File Shares	✓	✓	✓	✓	!	!	!	!
OneDrive	✓	✓	✓	✓	✗	✗	✗	✗
SharePoint	✓	✓	✓	✓	!	!	!	!
Teams	✓	✓	✓	✓	!	!	!	!
Email	✓	✓	✓	✓	✗	✗	✗	✗
Other M365 Apps	✓	✓	✓	✓	✗	✗	✗	✗
JMU Managed Workstation	✓	✓	✓	✓	✗	✗	✗	✗
Portable Storage	✓	!	!	!	✗	✗	✗	✗
Non-Microsoft Cloud Storage (e.g. Dropbox, Google)	✗	✗	✗	✗	✗	✗	✗	✗

**Research containing highly confidential data. All other research data should follow requirements for protected and public data.*

Legend	
✓	**Use Permitted** – Use of this storage option is acceptable and should be utilized in accordance with university policies.
!	**Use Restricted** – Use of this storage option with this data type is restricted and requires specific approval from JMU Information Technology to be used for storage or sharing. Approval may be requested by submitting a General Technology Solution Request.
✗	**Use Prohibited** – Use of this storage option with this data type is strictly prohibited and should not be used for storage or sharing.

2. Overview of Available Services

JMU File Shares (N: and other lettered drives): On-premise file storage for individuals and departmental groups. The JMU file shares are directly managed by JMU Information Technology (IT) and provide basic document sharing and backup/recovery capabilities. Access to other groups/department shares can be made available upon request.

Highly Confidential Data may be stored on JMU File Shares with assistance from IT.

See File Storage (N:Drive) at JMU for more information.

OneDrive: Cloud service in M365 that is for individual storage of public or protected data. Each employee receives 1 TB of individual storage. Students and affiliates receive 100 GB of individual file storage. Students, employees, and affiliates may share documents, files, and/or folders with users inside and outside of the University using the service.

Highly Confidential Data is prohibited from being stored in OneDrive.

See OneDrive at JMU for more information.

SharePoint: File management space in Microsoft 365 that is shared and used among groups of individuals or teams that require access to the same files. Because a SharePoint site is automatically created when a team is created in Microsoft Teams, IT recommends that users utilize file storage through Microsoft Teams. Each SharePoint site receives 500 GB of storage and additional storage may be requested as needed.

Highly Confidential Data may be stored in SharePoint with specific approval and assistance from IT.

See SharePoint at JMU for more information.

Teams: Microsoft Teams is the primary collaboration and productivity tool in Microsoft 365. It provides an easy-to-use interface that utilizes both the OneDrive and SharePoint technologies. With Teams, users can chat with individuals or groups, hold video meetings, make audio/video calls, store and share files, and integrate with other M365 applications. Each team has a backend SharePoint site with 500 GB of file storage and additional storage may be requested as needed.

Highly Confidential Data may be stored in Microsoft Teams with specific approval and assistance from IT.

See Microsoft Teams at JMU for more information.

Email: The JMU-managed Microsoft email system for employees and affiliates that includes email, calendar, and contact management services.

Highly Confidential Data is prohibited from being transmitted or stored in email.

See JMU Email (Faculty / Staff / Affiliates) for more information.

Other M365 Apps: Microsoft 365 apps (such as Planner, Forms, Loop, Lists, Bookings, and others) that are available to JMU employees when logged in to Microsoft 365.

Highly Confidential Data is prohibited from being used in these applications.

See Microsoft 365 at JMU for more information.

JMU Managed Workstation: An employee's computing environment and hard drive on a JMU managed computer, such as a desktop, laptop, or tablet.

Highly Confidential Data is prohibited from being stored on a JMU managed workstation.

Portable Storage: A USB flash drive, external hard drive, memory card, or other portable storage device.

Highly Confidential Data is prohibited from being stored on a portable storage device. Protected Data should not be stored on a portable storage device without specific approval from IT.