SUBJECT: **Information Technology**
PROCEDURE: **706.1.1 Data Stewardship**
EFFECTIVE: April 2024 **REVISED**: **REVIEWED**:

Introduction and Purpose

These standards establish minimum guidelines for the management and protection of institutional data as outlined in the four-campus data stewardship policy.

Data Classification

There are 3 classifications of college data. Data stewards have responsibility for classifying data in their areas and applying appropriate controls as described in this document.

CONFIDENTIAL DATA: *All* data which, if released in an uncontrolled fashion, could have substantial fiscal or legal impacts on the college. Examples include social security numbers, financial account numbers, driver's license numbers, health insurance policy ID numbers, and protected health information (PHI).

RESTRICTED DATA: *All data for which release or modification without authorization could adversely affect the operations, assets, or reputation of the college.* Examples include employee and student ID numbers (GIDS), course evaluations, financial transactions that do not include confidential data, contracts, planning documents, and student education records as defined by the Family Educational Rights and Privacy Act (FERPA). All files are assumed to be 'restricted' unless otherwise classified as 'public' or 'confidential.'

PUBLIC DATA: *All* data that is not restricted by one of the above classifications may be released to the general public in a controlled manner, such as information designated as "directory information" under college policy pertaining to FERPA. Other examples include course schedules, public web pages, campus maps, policy documents, faculty publications, job opening announcements and press releases.

Data Storage

In all cases, it is expected that data will be stored on IT (Information Technology) managed servers or approved hosted services, **not desktop systems**. Central servers will adhere to the latest security and performance practices for the operating system, hardware, and software. Great Falls College MSU IT servers are classified as 'managed' or 'secure' servers. The secure servers have a higher level of security requirements, encryption, and connectivity. Storage of *Confidential Data* outside of specified IT secure server storage space is **prohibited.**

Storage of *Restricted Data* outside of IT secured servers or approved hosted services is **prohibited** unless authorized per a documented discussion with the appropriate Data Steward and the director of IT.

Furthermore, servers housing *Restricted Data* will conform to the above guidelines and employ the following additional controls:

- Data will be encrypted through standard encryption techniques.
- Authorized users will gain access through encrypted authentication and multi factor authentication (MFA) whenever possible.
- Transmission of data between client and server will be encrypted whenever possible without introducing additional security risks.
- Access must be authorized by the Data Steward (or their designate).

- All data and system access will be logged and preserved for at least 8 weeks (about 2 months).

Restricted data, excluding FERPA-protected information such as materials associated with search committees, may be stored on IT managed servers or an approved hosted solution. Contact Information Technology office for analysis and determination of appropriate use of such managed servers.

While *Public Data* may be stored on local desktop hard drives and removable media, this practice is **not advised** as it carries risk of data loss due to hardware failure.

Use the following table to choose the right location for the data you need to store.

Data Type	OneDrive for Business / SharePoint	Knox	DocuSign	Email
Budget information	**Yes**	**No**	**Yes**	**Yes**
Contracts	**Yes**	**No**	**Yes**	**Yes**
Course evaluations	**Yes**	**No**	**Yes**	**Yes**
Data classified as *Public*	**Yes**	**No**	**Yes**	**Yes**
Data classified as *Restricted*	**Yes**	**Yes**	_*Yes*_	**No**
Employee and student IDs/GIDs (even when combined with names)	**Yes**	**Yes**	_*Yes*_	**No**
Planning documents	**Yes**	**No**	**Yes**	**Yes**
Staff search committee notes	**Yes**	**No**	**Yes**	**Yes**
Student grades and records	**Yes**	**Yes**	_*Yes*_	**No**
Bank account numbers	**No**	**Yes**	_*Yes*_	**No**
Credit card numbers	**No**	**No**	**No**	**No**
Data classified as *Confidential*	**No**	**Yes**	_*Yes*_	**No**
Drivers license numbers	**No**	**Yes**	_*Yes*_	**No**
Passport Visa numbers	**No**	**Yes**	_*Yes*_	**No**
Payroll ACH numbers	**No**	**Yes**	_*Yes*_	**No**
Social Security numbers	**No**	**Yes**	_*Yes*_	**No**

Note that college-managed Teams/OneDrive accounts may be used for storage of *Restricted Data* including education records as defined by FERPA. Use of other cloud storage solutions, such as Google Docs or Dropbox, has not been approved by the college for storage of FERPA restricted data.

Additionally, note that college data stored in non-college cloud services are subject to Great Falls College data stewardship standards. It is the data user's responsibility, with the data steward, to ensure that proper controls and practices are in place and to receive approval for all implementations, operations, and changes from the director of IT.

Data Sharing

Public Data may be shared through any means including managed file services, publicly available web servers, and college email accounts.

Sharing of confidential and restricted data, when necessary, will be done through managed accounts on servers managed as described above. Sharing and distribution of data can be accomplished in the following ways:

- Managed file services: Managed file services are systems that are managed locally and help you transfer and store files using standard technologies. Confidential data must be encrypted when it is being transferred and when it is stored, unless other security measures are in place and approved by the director of IT.
- Managed Web Services: This includes hosted solutions including Desire2Learn, OneDrive or other college-approved systems. Web services hosting *Confidential* or *Restricted Data* will employ secure communications via HTTPS and encrypted authentication for authorized users. Email may not be used for the distribution or sharing of *Confidential* or *Restricted Data.* The Data Steward (or their delegate) will be responsible for authorizing access to all *Confidential* and *Restricted Data* within a managed web service.

Data Reporting

Information is typically extracted from central repositories for reporting purposes. Reporting considerations include:

- Reports should be handled in accordance with the above guidelines (i.e., reports with *Confidential* or *Restricted* information should not be distributed via email or stored on local desktops).
- Administrative reporting should be accomplished through central systems managed by the IT office.
- Reports should contain only the information needed to meet functional requirements. *Confidential* or *Restricted* information should be contained in reports only when deemed necessary and approved by the appropriate data steward.
- Access to Banner data by persons without direct Banner authorization to Banner data will be vetted through the IT office and data steward and follow the data access agreement.

<u>Definitions</u>

<u>Data steward</u>: college officials who have responsibility for data within their functional areas. Ultimate authority for stewardship of college data rests with the CEO/Dean, though it is typically delegated to the respective steward along with the director of IT.

<u>Data users</u>: individuals, including faculty, staff, administrators, and students, who use college data as part of their assigned duties or in fulfillment of their roles or functions within the college community.

Data administration: the function of applying formal guidelines and tools to manage the college’s information resource. The responsibility for data administration is shared among the data stewards, data users and information technology personnel.

Computer system administration: the function of maintaining and operating hardware and software platforms (systems). Responsibility for the activities of computer system administration belongs to IT.

Application administration: the function of developing and maintaining applications and software. Responsibility for the activities of application administration belongs to IT. Delegated authority may be granted to other divisions or departments within the college by the director of IT.