DATA STEWARDSHIP STANDARDS

Policy: Enterprise Data Stewardship Policy
Document: Data Stewardship Standards
Campus: MSU Billings (MSUB)
Revision: 08/22/23
Contact: Chair of Data Governance Council

These Standards establish minimum guidelines for the management and protection of institutional data as outlined in the University Data Stewardship Policy (http://www.montana.edu/policy/enterprise_it/data_stewardship.html).

Data Stewardship Roles and Responsibilities

DATA STEWARDS are University officials who have delegated responsibility and authority for the validity, use, and dissemination of defined data within their functional areas. Delegated authority and responsibility to the data stewards is granted by the Chancellor, as defined in the University Data Stewardship Policy.

The university system Campus Data Stewards can be found at https://www.montana.edu/datagovernance/secure/datastewards.html.

DATA USERS are individuals, including faculty, staff, administrators, and students, who use institutional data as part of their assigned duties or in fulfillment of their roles or functions within the University community.

DATA ADMINISTRATION is the function of applying formal guidelines and tools to manage institutional data. The responsibility for data administration is shared among the data stewards, data users, and information technology (IT) personnel.

INSTITUTIONAL DATA are data elements which are created, received, maintained and/or transmitted while meeting the institution's administrative and academic requirements. Institutional Data can be:

1. Contained in any form, including but not limited to documents, databases, spreadsheets, email, and websites;
2. Represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof;
3. Communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and
4. Recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other information systems.

Data Classification

There are three classifications of institutional data. Data Stewards have the 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 University. Examples include social security numbers, financial account numbers, driver's license numbers, health insurance policy ID numbers, protected health information (PHI), passport visa numbers, and export-controlled information under U.S. laws.

RESTRICTED DATA: All data for which release or modification without authorization could have an adverse effect on the operations, assets, or reputation of the University. 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) (http://www.msubillings.edu/stuaff/ferpastudents.htm/). 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 and may be released to the general public in a controlled manner, such as information designated as "Directory Information" under university 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 required that data will be stored on IT managed servers or approved hosted services, not desktop or laptop systems. Managed servers will adhere to the latest security and performance practices for the operating system, hardware, and software. The storage of *Confidential Data* outside of IT managed servers is strictly prohibited.

Storage of *Restricted Data* outside of IT managed servers or approved hosted services is prohibited unless authorized per a documented discussion with the MSUB Data Governance Council. Contact the Office of Information Technology for analysis and determination of appropriate use of such managed services.

Storage of Public data shall also be limited to either IT managed servers or approved hosted services, not desktop or laptop systems.

Access to confidential or restricted data must be authorized by the Data Steward (or their designee). All data and system access will be logged, and logs will be preserved for a minimum of 8 weeks.

The use of removeable media (thumb drives, external hard drives, DVDs, etc.) is highly discouraged due to the risk of data loss due to hardware failures and lost or stolen media.

Permissible storage solutions for each Data Classification are as follows:

Data Type	Box or OneDrive	SharePoint Online	IT Managed Servers
Public	**Yes**	**Yes**	**Yes**

Restricted	**Yes**	**Yes**	**Yes**
Confidential	**No**	**No**	**Yes**

Where: "Box" refers to University-managed storage accounts on box.com.
Where: "OneDrive" refers to University-managed storage accounts on Office 365.
Where: "SharePoint Online" refers to SharePoint storage locations within Office 365.
Note that University-managed Box/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, are not approved for storage of any institutional data.

Institutional data stored in cloud services are subject to MSUB Data Stewardship Standards defined in this document. It is the responsibility of the Data User, in conjunction with the Data Steward, to present the use of the cloud service and the data being utilized to the Data Governance Council for review to ensure that proper controls and practices are in-place. Information about the Data Governance Council Project Review Workflow can be found on the MSUB Intranet (https://www.msubillings.edu/intranet/data-governance-council/). Additionally, an Enterprise Data Request (https://www.montana.edu/datagovernance/secure/datarequests.html) must be submitted for review and approval for all implementations.

Storage of payment card data is not addressed in this document. For guidance on handling of information subject to Payment Card Industry Data Security Standards (PCI-DSS), please see *Safeguarding Customer Information* at: http://www.msubillings.edu/boffice/safeguarding.htm.

While most research data are classified as Restricted Data, storage, backups, and proper data identification is the responsibility of the Data User in collaboration with the Data Steward and Data Governance Council.

Data Sharing

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

Sharing of *Confidential* and *Restricted Data,* when necessary, will be accomplished through the use of managed accounts on servers managed as described above. Sharing and distribution of data can be accomplished in the following ways:

- Managed file services: This includes locally managed systems providing file transfer and storage services using standard technologies such as SMB, SFTP, and WebDAV. Confidential data must be encrypted in transit unless other mitigating controls are in-place and approved by the Chief Information Officer.

- Managed Web services: This includes hosted solutions including Desire2Learn, Box, or other University-approved systems. Web services hosting *Confidential Data* 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 Data* or *Restricted Data.* The Data Steward (or their designee) 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 or laptop systems).

- Administrative reporting should be accomplished through Institutional Research approved systems, such as Tableau, that are managed by the Office of Information Technology and approved for sharing data.

- Reports should contain only the information needed to meet functional requirements. *Confidential* or *Restricted* information should be contained in reports only when deemed absolutely necessary and approved by the appropriate Data Steward. Additionally, any data publicly released shall come from centralized systems. Redisclosure of information for another purpose is not permissible.

- Access to Banner data by persons without direct Banner authorization to Banner data will be vetted through the Data Governance Council and Data Steward and follow the Data Access Agreement.

Data Disposal

Prior to repurposing or recycling, all electronic information stored on any device will be properly purged. This includes internal and external storage devices and removable media.

Guidelines for the retention and disposition of records, created or maintained in the course of university business, can be found in the Montana University System General Record Retention Schedule (https://mus.edu/che/directives/GerenalRecordRetentionSchedule.pdf). Guidelines for proper handling of surplus computing equipment are addressed in Montana Board of Regents of Higher Education Information Technology Policy 1308 – Disposal of Computer Storage Devices (https://mus.edu/borpol/bor1300/1308.pdf).

Paper reports containing *Confidential* or *Restricted* Information will be shredded prior to disposal. A cross-cut shredder is recommended.

MSUB ID (GID) Standards

Appropriate use, storage, and sharing of the MSUB identifier (MSUB ID), also known as the GID, requires further explanation and clarification. The following section outlines Restricted Data guidelines for the GID, clarifies the current GID standards and procedures, and discusses how to request an exception for use and/or storage of the GID.

As indicated above, restricted data may not be sent through email. However, full GIDs can be emailed if the names, email, addresses or other identifying information are not present in the email. Additionally, partial GID (last 4 numbers) can be sent through email with the name of the

individual to whom it belongs.

Storage of GID Numbers

GIDs numbers must be stored on IT managed servers or approved hosted services, not desktop or laptop systems. The Data Governance Council must be consulted to identify approved third-party storage. Proper management of GID numbers includes compliance with the Technology Management Policy (https://www.montana.edu/policy/enterprise_it/technology_management.html).
Storage of GIDs outside of IT managed servers or approved hosted services (like Box) is prohibited unless authorized per a documented discussion with the appropriate campus Data Steward and campus Chief Information Officer. Furthermore, servers housing GIDs will conform to the above guidelines and employ the following additional controls:

- Data will be encrypted by using database or file system encryption techniques where possible.
- Authorized users will gain access through encrypted authentication with their NetID/password.
- Transmission of data between client and server will be encrypted where possible.
- A plan for authorizing access for users must be approved by the campus Data Steward (or their designee).
- All system access will be logged, and logs will be preserved for a minimum of 8 weeks.

MSUB ID (GID) Exceptions

To request an exception to the current MSUB ID (GID) Standard, the user must complete an MSUB ID (GID) Request Exception Form found at https://www.msubillings.edu/intranet/data-governance-council/files/MSUB_GID_Request_Exception_Form.docx.