DATA STEWARDSHIP STANDARDS

Policy: Enterprise Data Stewardship Policy
Document: Data Stewardship Standards
Campus: MSU-Billings (MSUB)
Revision: 03-12-18
Contact: Michael Barber, Chief Information Officer
mbarber@msubillings.edu

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 responsibility for data within their functional areas. Ultimate authority for stewardship of University data rests with the Chancellor, though is typically delegated to the respective steward along with the Chief Information Officer (CIO) and/or Legal Counsel as defined in the University Data Stewardship Policy.

DATA USERS are individuals, including faculty, staff, administrators, and students, who use University 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 the university's information resource. The responsibility for data administration is shared among the data stewards, data users, and information technology personnel.

COMPUTER SYSTEM ADMINISTRATION is the function of maintaining and operating hardware and software platforms (systems). Responsibility for the activities of computer system administration belongs to the Office of Information Technology. Delegated authority may be granted to other divisions or departments within the University by the Chief Information Officer.

APPLICATION ADMINISTRATION is the function of developing and maintaining applications and software. Responsibility for the activities of application administration belongs to the Office of Information Technology. Delegated authority may be granted to other divisions or departments within the University by the Chief Information Officer.

Data Classification

There are 3 classifications of University 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 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 expected that data will be stored on IT 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. MSU Billings 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 Chief Information Officer.

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

- Data will be encrypted through the use of database or file system encryption techniques whenever possible.
- Authorized users will gain access through encrypted authentication.
- 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 logs will be preserved for a minimum of 8 weeks.

Restricted data, may be stored on IT managed servers or an approved hosted solution. Contact the Office of Information Technology 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.

Permissible storage solutions for each Data Classification are as follows:

Data Type	Hard drive or Removable Media	Box or OneDrive	SharePoint On Campus	SharePoint Online	MSUB IT Managed Servers	MSUB IT Secured Servers
Public	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**No**
Restricted	**No**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Confidential	**No**	**No**	**No**	**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**.

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, have not been approved by The University for storage of FERPA restricted data.

Additionally, note that University data stored in non-MSUB cloud services are subject to MSUB Data Stewardship Standards. It is the responsibility of the Data User, in conjunction with the Data Steward, to ensure that proper controls and practices are in-place and to receive approval for all implementations, operations, and changes with the CIO.

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

Storage and backups of research data, while most research data are classified as *Restricted*, proper data identification and storage is the responsibility of the Data User in collaboration with the Data Steward and CIO.

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 and at rest 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* 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 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 Office of Information Technology.

- 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.

- Access to Banner data by persons without direct Banner authorization to Banner data will be vetted through the Office of Information Technology 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 hard drives and removable media. 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

The University has established minimum guidelines for the management and protection of institutional data. These guidelines are outlined above. The MSUB identifier, known as the GID, requires further explanation and clarification. The following outlines *Restricted Data* guidelines, clarifies the current MSUB ID (GID) standards and procedures, and discusses how to request an exception for use and/or storage of the MSUB ID (GID).

Data Classification – Restricted Data

There are three classifications of University data: *Confidential, Restricted and Public*. *Restricted data* is defined as all data for which release or modification without authorization could have an adverse effect on the operations, assists or reputation of the University. Examples include: Employee and Student ID numbers (MSUB IDs). The current MSUB ID (GID) Standard is listed below:

Current MSUB ID (GID) Standard

1. Full GIDs can be emailed if the names, email, addresses or other identifying information are not present in the email.
2. Partial GID (last 4 numbers) can be sent with name.

Storage of MSUB IDs (GID)

MSUB IDs (GIDs) must be stored on Centrally Managed IT Servers or Approved Hosted Servers, not desktop systems. The campus CIO will be consulted to identify approved third party storage. Proper management of MSUB ID (GID) includes compliance with the Technology Management Policy.

Storage of *Restricted Data* MSUB IDs (GIDs) outside of centrally 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 *Restricted Data* will conform to the above guidelines and employ the following additional controls:

- Data will be encrypted by using database or file system encryption techniques.
- Authorized users will gain access through encrypted authentication.
- Transmission of data between client and server will be encrypted without introducing security risks.
- Access must be authorized by the campus Data Steward (or their designate).
- All data and system access will be logged, and logs will be preserved for a minimum of 8 weeks.

Data Reporting – Restricted Data

Reports should be handled in accordance with above guidelines (i.e reports with *Confidential* or *Restricted* information should not be distributed via email or stored on local desktops).

MSUB ID (GID) Exceptions

To request an exception to the current MSUB ID (GID) Standard, the user will need to complete an MSUB ID (GID) Request Exception Form.

MSUB ID (GID) Request Exception Form

Please complete the following form to request an MSUB ID (GID) use exception. Exception requests will be reviewed by the campus CIO and Data Governance Council.

1. Provide your contact information:
    a. Department:
    b. Contact:
    c. Email:
    d. Phone

2. What is the business justification for not following the current MSUB ID (GID) Standard?

3. Describe how you will be using the MSUB ID (GID)?

4. What is the duration you need the exception?
    a. Start Date:
    b. End Date:

5. What is the number of MSUB IDs (GIDs) being used?

6. Please identify alternative solutions that have been considered (e.g. sharing MSUB IDs in Box).

7. Please identify compensating controls that will be in place to provide confidentiality of MSUB IDs (GIDs) if the exception is approved.