ENTERPRISE IT STANDARDS AND PROCEDURES:
DATA STEWARDSHIP STANDARDS

Document: Data Stewardship Standards
Campus: MSU-Northern
Revised Date: May 2018
Review Date: May 2020
Contact: Chief Information Officer

These Standards establish minimum guidelines for the management and protection of institutional data as outlined in the Montana State University Enterprise Data Stewardship Policy.

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 president, though is typically delegated to the respective steward along with the Chief Information Officer and/or Legal Counsel as defined in the 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 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). All files are assumed to be '*restricted*' unless otherwise classified as '*public*' or '*confidential*'.

See the *Employee and Student ID Number (GID) Standards* section later in this document for additional guidelines regarding the use and storage of GIDs.

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.

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 contact the MSU-Northern Business Services.

Storage and backups of research data are not addressed in this document. While most research data are classified as *Restricted*, proper data identification and storage is the responsibility of the Data User with guidance from the Data Steward and Chief Information Officer.

Data Storage

In all cases, it is expected that *Confidential* and *Restricted* data will be stored on servers managed by Information Technology Services (ITS) or on approved hosted services, not desktop or mobile systems, or any unencrypted portable data storage devices. Proper management includes compliance with the MSU Enterprise Technology Management Policy.

Storage of *Confidential Data* outside of Sulafat is prohibited. Where: "Sulafat" refers to the ITS-managed server sulafat.msun.edu.

Storage of *Restricted Data* outside of centrally managed 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.

A subset of *Restricted* data, **not including** FERPA-protected information, such as materials associated with search committees, may be stored on managed servers such as Rigel. Where: "Rigel" refers to the ITS-managed fileserver, rigel.msun.edu. Please contact the Information Technology Services 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:

	Hard Drive or Removable Media	Rigel	Box/OneDrive	Sulafat
Public Data	✓	✓	✓	✖
Restricted Data	✖	✓	✓	✓
Confidential Data	✖	✖	✖	✓

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-MSU approved cloud services are subject to MSU 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.

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 on disk unless other mitigating controls are in-place and approved by the Chief Information Officer (or designee).

- Managed Web services: This includes hosted solutions including Desire2Learn, Box, OneDrive, 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 Confidential or Restricted Data. The Data Steward (or their delegate) will be responsible for authorizing access to all *Confidential* and *Restricted Data*.

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 Banner or Argos systems whenever possible.

- 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.

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.

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

Employee and Student ID Number (GID) Standards

The following section outlines *Restricted Data* guidelines for the employee and student ID numbers (GIDs), clarifies the current GID standards and procedures, and how to request an exception for use and/or storage of GIDs.

- As stated above in the Data Sharing section, 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.
- Partial GID (last 4 numbers) can be sent through email with the name of the individual to whom it belongs.

Storage of GIDs

GIDs must be stored on Centrally Managed ITS Servers or Data Governance Council Approved Hosted Servers, **not desktop systems**. The campus CIO will be consulted to identify approved third party storage. Proper management of GIDs includes compliance with the MSU Enterprise Technology Management Policy.

Storage of GIDs outside of centrally managed servers or approved hosted services (like Box) is prohibited unless authorized per a documented formal request for an exception. 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.

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

Request for GID Standards Exception(s)

To request an exception to the current GID Standards, the user will need to complete the Employee and Student ID Number (GID) Exception Request Form and submit it to the campus CIO for approval and routing.