ENTERPRISE IT STANDARDS AND PROCEDURES

DATA STEWARDSHIP STANDARDS

Policy:	**Enterprise Data Stewardship Policy**
Document:	**Data Stewardship Standards**
Campus:	**MSU-Bozeman**
Revision:	**3.3**
Contact:	**Justin van Almelo | CISO** **justin.vanalmelo@montana.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).

1.0 Data Stewardship Roles and Responsibilities

1.1 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 CIO and/or Legal Counsel as defined in the Policy (http://www.montana.edu/policy/enterprise_it/data_stewardship.html).

1.2 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.

1.3 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.

1.4 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 Information Technology Center with delegated authority to other divisions or departments within the University.

1.5 APPLICATION ADMINISTRATION is the function of developing and maintaining applications and software. Responsibility for the activities of application administration belongs to the Information Technology Center with delegated authority to other divisions or departments within the University.

2.0 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.

2.1 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.

2.2 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 (GID / MSU ID), 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.montana.edu/policy/family_ed_privacy_act/). All files are assumed to be 'restricted' unless otherwise classified as 'public' or 'confidential'. More detailed information about appropriate use, storage, and sharing of student ID numbers (GID / MSU ID), can be found in section 7.0 of this standards document.

Please note, that employee and student ID numbers, (GIDs) are referred to by different names on each MSU campus. They shall, however, be handled in accordance with these standards regardless of the campus affiliation of the individual to whom the ID number belongs.

2.3 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 and per procedures, 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.

3.0 Data Storage

In all cases, it is expected that data will be stored on managed servers or approved hosted services, not desktop systems. Proper management includes compliance with the Technology Management Policy

3.1 Storage of *Confidential Data* outside of Knox or DocuSign is prohibited. Where: "**Knox**" refers to the ITC-managed server **knox.montana.edu** and DocuSign refers to .

3.2 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 Security Officer. Furthermore, servers housing *Restricted Data* will conform to the above guidelines and employ the

following additional controls:

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

3.3 A subset of restricted data, not including FERPA-protected information such as materials associate with search committees, may be stored on managed servers such as **Opal**. Where: "**Opal**" refers to the ITC-managed fileserver, **opal.msu.montana.edu**. Please contact the Information Security Group for analysis and determination of appropriate use of such managed servers.

3.4 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.

3.5 Permissible storage solutions for each Data Classification are as follows:

	Hard Drive or Removable Media	Opal	Box/OneDrive	DocuSign	Knox
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**.

3.6 Note that University-managed Box/OneDrive accounts or DocuSIgn forms 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.

3.7 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.

3.8 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 University Business Office or reference the MSU Business Procedures Manual.

3.9 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, Vice-President of Research and Economic Development.

4.0 Data Sharing

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

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

4.2 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 Security Officer or their designee.

4.3 Managed Web services: This includes hosted solutions including Desire2Learn, Box, OneDrive, DocuSign, or other University-approved systems. Web services hosting *Confidential* or *Restricted Data* will employ secure communications via HTTPS and encrypted authentication for authorized users.

4.4 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.*

5.0 Data Reporting

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

5.1 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).

5.2 Administrative reporting should be accomplished through central Banner or Argos systems whenever possible.

5.3 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.

6.0 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: http://www.mus.edu/borpol/bor1300/1308.htm

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

7.0 MSU ID (GID) Standards

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

7.1 As indicated in section 4.4, 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.

7.2 Partial GID (last 4 numbers) can be sent through email with the name of the individual to whom it belongs.

7.3 Storage of MSU IDs (GID)

7.3.1 MSU IDs (GIDs) must be stored on Centrally Managed Servers or Approved Hosted Servers, not desktop systems. The authorized party must be specifically identified who can approve hosted servers. Proper management of MSU ID (GID) includes compliance with the Technology Management Policy.

7.3.2 Storage of MSU 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 MSU IDs (GIDs) will conform to the above guidelines and employ the following additional controls:

7.3.2.1 Data will be encrypted by using database or file system encryption techniques.

7.3.2.2 Authorized users will gain access through encrypted authentication with their NetID/password.

7.3.2.3 Transmission of data between client and server will be encrypted.

7.3.2.4 A plan for authorizing access for users must be approved by the campus Data Steward (or their designate).

7.3.2.5 All system access will be logged and logs will be preserved for a minimum of 8 weeks.

7.7 MSU ID (GID) Standards: Request for Exceptions

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

MSU ID (GID) Request Exception Form

<table>
<tr><td colspan="2">Please complete the following form to request an MSU ID (GID) use exception. Exception requests will be reviewed by the MSU Data Security, the campus-specific Data Steward(s) and the Data Governance Council.</td></tr>
<tr><td>Campus and Department:</td><td>Contact Name:</td></tr>
<tr><td>Email:</td><td>Phone:</td></tr>
<tr><td colspan="2">What is the business justification for not following the current MSU ID (GID) standard?</td></tr>
<tr><td colspan="2">Describe how you will be using the MSU ID (GID)?</td></tr>
<tr><td colspan="2">Describe if/how you are improving processes to comply with the MSU ID (GID) standards for your campus.</td></tr>
<tr><td colspan="2">What is the duration you need the exception?

Start Date: End Date:</td></tr>
<tr><td>Type of MSU ID (GID):</td><td>Exception Status:</td></tr>
<tr><td colspan="2">Signatures:</td></tr>
<tr><td colspan="2">Requestor:</td></tr>
<tr><td colspan="2">Enterprise Data Security:</td></tr>
</table>

Enterprise PMO:
Campus Data Steward(s):
DGC Review date: