

# Data Stewardship Guidelines

*June 2007*

## INTRODUCTION

The following Data Stewardship Guidelines recognize data as a university asset which, like other resources, must be managed with overall utility and cost/benefit in mind. Based on the philosophy that the greatest benefit of data is gained through its shared and thoughtful use but diminished through loss, misuse, misinterpretation and unnecessary restrictions to its access, these guidelines establish minimum standards for the management and protection of institutional data as provided in the University Data Stewardship Policy ([http://www2.montana.edu/policy/itc/data\\_stewardship.htm](http://www2.montana.edu/policy/itc/data_stewardship.htm)). It is designed to achieve an appropriate mix of three core values – confidentiality, integrity and availability - which are described below along with the associated assumptions under which MSU's data repositories shall be administered and used.

- Confidentiality. University data should be available to meet the legitimate needs of members of the University community including access to sensitive information maintained in University data repositories. It is understood, however, that some data may be subject to legal and ethical considerations which define and regulate its responsible use. Provisions to not only increase the University community's understanding of the data and to maximize sensitivity to appropriate uses of all information, especially information that is considered "confidential," should be central to the university's data stewardship model. Controls must be in place to minimize the risk of unauthorized disclosure of university data.
- Integrity. The university community should trust the integrity of institutional data. Data should be collected and maintained, therefore, to guarantee its consistency, reliability, timeliness and accuracy and to avoid duplication and disparity across databases. Appropriate security measures should be provided which will protect institutional data from compromise or unauthorized access, modification, destruction or disclosure. Individuals share responsibility and are accountable for their use and access of the university's data repository, requiring on-going education on the part of those who use and care for it.
- Availability. This document provides guidelines and procedures which will support ease of use and access to data according to the authorized and legitimate needs of members of the University community. For purposes of this document, legitimate access is further defined as access which provides information necessary for users to carry out assigned duties or to fulfill a role or function. Additionally, the controls described here ensure that data will be available when needed.

## **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 CIO and/or Legal Counsel as defined in the Policy ([http://www2.montana.edu/policy/itc/data\\_stewardship.htm](http://www2.montana.edu/policy/itc/data_stewardship.htm)).

DATA MANAGERS are individuals, including faculty, staff, administrators who typically guide the collection, storage, and sharing of University information. The Data Manager will answer to the Data Steward on matters related to information handling.

DATA USERS are individuals, including faculty, staff, administrators and students, who need and 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. Responsibility for activities of 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 (system environments). Responsibility for the activities of computer system administration may belong to the Information Technology Center or to other divisions or departments within the University. Individuals with administrative or root access to systems housing University data fall into this category.

APPLICATION ADMINISTRATION is the function of developing and maintaining application and software environments. Responsibility for the activities of application administration may belong to the Information Technology Center or to other divisions or departments within the University. Individuals with administrative access to University applications fall into this category.

### **DATA CLASSIFICATION**

The University Data Stewardship Policy and section 510.20 of the University Data Security Policy describe the 4 classifications of University data. Data Stewards and Data Managers have responsibility for classifying data in their areas and applying the applicable controls as described in this document. The definitions and responsibilities for these classifications are provided below:

Restricted Data: All data which, if released in an uncontrolled fashion, could have substantial fiscal or legal impacts on the University. Examples include personal data containing elements such as Social Security Numbers, student grades, and personnel records. Personally identifiable information (other than public directory information as

defined under FERPA: [http://www2.montana.edu/policy/family\\_ed\\_privacy\\_act](http://www2.montana.edu/policy/family_ed_privacy_act)) should be considered *Restricted*.

External Data: All data belonging to an outside party or agency. Examples include data maintained by commercial account owners and certain researchers who have special data arrangements with public or personal agencies. Access control is the responsibility of the local owners and researchers, who may request assistance in securing data from the Enterprise Security Manager.

Personal Data: All data equivalent to personal documents stored in desks or file cabinets. Examples include electronic mail, personal correspondence, and personal files, including most research files. Access control is the responsibility of each individual account owner, who may request assistance in securing data from the Enterprise Security Manager (Section [510.50](#)). Recipients of *Restricted Data* are responsible for maintaining the restricted nature of the data in accordance with these guidelines which precludes local storage in most cases.

Public Data: All data that is not restricted by one of the above classifications and may be released to the general public, such as information designated as "Directory Information" under University policy pertaining to the Family Educational Rights and Privacy Act. Availability and integrity of this information is the responsibility of the appropriate application administrator.

## **DATA STORAGE**

The requirement to store University data exists for each data type defined above. In all cases, it is expected that data will be stored on managed servers, not desktop systems. Proper management includes compliance with the Standards for Network Connectivity (<http://www.montana.edu/itac/campusnetstds.doc>) which includes but is not limited to the following practices:

- Operating Systems with current support will be used
- All currently available and applicable patches will be tested and installed in a timely manner
- Unnecessary services will be disabled
- A properly configured firewall will be enabled
- Vulnerability scans will be performed on a regular basis
- System and access logs will be monitored or reviewed on a regular basis
- Automated backups to removable media will be configured and tested on a regular basis
- Automated backup media will be managed and stored securely by responsible personnel in a location separate from the server.
- Access will be controlled through a managed authentication/authorization system (such as the Windows Active Directory) with appropriate permissions limited to those as required

- Administrative access will be limited to the system and/or application administrator as required
- Hardware will be housed in a physically secure environment with access restricted to authorized personnel. The environment will include redundant power and cooling, and suitable fire suppression whenever feasible.

Storage of *Restricted Data* outside of centrally managed servers is discouraged and should only be undertaken when absolutely necessary. It is expected that the decision to store *Restricted Data* in this manner will occur only after discussion with the appropriate Data Steward and ITC personnel. 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 sensitive data between client and server will be encrypted
- 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

The use of removable media (other than for managed backups) is typically discouraged for the storage of *Restricted Data*. When necessary, *Restricted Data* must be encrypted when stored on portable devices such as USB drives, desktops, or laptop computers.

#### **DATA SHARING**

Data sharing will be accomplished through the use of managed accounts on servers managed as described above based on functional job requirements. Sharing and distribution of data can be accomplished in the following ways:

- Managed file services. This includes systems providing file shares through SMB or comparable protocols
- Managed Web services. This includes the use of the MyMSU portal, WebCT, or other similar systems.
  - Web services hosting *Restricted Data* will employ secure communications via HTTPS and encrypted authentication or authorized users.

Email will not be used for the distribution or sharing of *Restricted Data*. The Data Steward (or their designate) will be responsible for authorizing access to *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 *Restricted* information should not be distributed via email or stored on local desktops)
- Administrative reporting should be accomplished through central Banner systems whenever possible
- Reports should contain only the information required to meet functional requirements. *Restricted* information should be contained in reports only when deemed 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 can be found here: <http://www2.montana.edu/desktop/surplus.htm>.

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

### **TRAINING**

It is expected that all individuals with responsibilities that include data handling will be properly trained in the procedures and best-practices commonly employed to protect information.

Formal Banner training is required as part of the authorization process in order to be granted access to the MSU Banner system. Training and access is coordinated through the Banner Module Team Leaders.

General training for individuals with IT-related support responsibilities is available through the ITC ITSS training program (<http://www.montana.edu/wwwitc/itsupport/>).

Departmental and one-on-one training on IT security and data stewardship is available through ITC and the Enterprise Security Manager.