

Data Classification Policy

Purpose

University enterprise-level administrative data are assets owned by Western Michigan University and must be protected accordingly. A data policy is necessary to provide a framework for securing data from risks including, but not limited to: access, use, disclosure, modification, removal, and destruction.

This policy serves as a foundation for the university's data classification security policies, and is consistent with the university's data and records management standards. The university recognizes that the value of its data and data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or to impede use for those individuals who use the data in support of university business or academic pursuits. This policy also serves to assure faculty, staff, and students that the expectation of privacy and confidentiality of their personal data will be maintained as outlined according to university policy and all state and federal laws and regulations.

All members of the university community have a responsibility to protect the confidentiality, integrity, and availability of data irrespective of the medium on which the data resides and regardless of format (such as, but not limited to: electronic, paper and any other physical form). Some examples of responsible data stewardship may include storing data in secured areas, not placing sensitive data on public web sites, proper disposition of antiquated data, strong passwords on computing devices, and utilizing adequate access control procedures.

Scope

This policy applies to all centrally managed university enterprise-level administrative data and to all user-developed data stores and systems that may access university data, regardless of the environment where the data reside including, but not limited to: mid-range systems, servers, desktop computers, laptop computers, USB keys, flash drives, and any other mobile computing device. The policy applies regardless of the media on which data reside including, but not limited to: electronic, microfiche, printouts, and CD, as well as the form the data may take including, but not limited to: text, graphics, video, and voice.

This Policy does not apply to Protected Health Information as defined by the Health Insurance Portability and Accountability Act (HIPAA) as such information shall be handled in accordance with the HIPAA Policies and Procedures adopted by the entity covered by HIPAA. Questions or concerns should be directed to the university HIPAA Privacy and Contact Officer currently located in the Office of the Vice President for Legal Affairs and General Counsel

Policy

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with the value, sensitivity, and risk involved.

To implement security at the appropriate level, to establish guidelines for legal/regulatory compliance, and to reduce or eliminate conflicting standards and controls, data will be classified into one of the following categories:

- **Restricted/Confidential:** data that, if disclosed to unauthorized persons, would be a violation of federal or state laws or, university policy, or university/contracts. Any file or data that contains personally identifiable information of a trustee, officer, agent, faculty, staff, retiree, student, graduate, donor, or vendor may also qualify as

restricted/confidential data. By way of illustration only, some examples of confidential data include, but are not limited to:

- Medical records of any kind
 - Student records (except for that information designated by the university as directory information under FERPA) and other non-public student data
 - Unique identifiers such as social security numbers or Western identification numbers
 - Certain Personnel records such as benefits records, health insurance information, retirement documents and/or payroll records
 - Any data identified by state or federal law or government regulation, or by order of a court of competent jurisdiction to be treated as confidential or sealed by order of a court of competent jurisdiction.
- **Internal:** internal data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be any law or other regulation requiring this protection. Internal data is information that is restricted to personnel designated by the university who have a legitimate business purpose for accessing such data. By way of illustration only, some examples of internal data include, but are not limited to:
 - Employment data
 - Business partner information where no more restrictive confidentiality agreement exists
 - Internal directories and organization charts
 - Planning documents
 - **Public:** data to which the general public may be granted access in accordance with Western Michigan University policy or standards. By way of illustration only, some examples of public data include, but are not limited to:
 - Publicly posted press releases
 - Publicly posted schedules of classes
 - Posted interactive university maps, newsletters, newspapers and magazines
 - Telephone directory information
 - Information posted on the university's public Web site including the web site for Student Academic and Institutional Research

Measures for data security are set by the data custodian working in conjunction with the data stewards, utilizing a combination of acceptable technology protocols and standards. Examples may include data encryption, data access controls, data retention and disposal procedures, data storage management, and end user training and awareness programs.

Responsibilities

The following roles and responsibilities are established for carrying out this data policy:

- **Data Trustee:** university officials (or their designees) who have planning and policy-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning Data Stewards, participating in establishing policies, and promoting data resource management for the benefit of the entire university. The Vice President for Business and Finance; Provost and Vice President of Academic Affairs; Vice Provost for Academic Operations and Chief Information Officer; and Registrar, are examples of Data Trustees.

- **Data Steward:** university officials having direct operational-level responsibility for information management (usually department directors). Data Stewards are responsible for data access and policy implementation issues. The Student Financial Aid and Scholarships Office, Admissions Department, Registrar's Office, Accounting Services, and Department of Human Resources, are examples of Data Stewards.
- **Data Custodian:** departments and/or personnel responsible for providing a secure infrastructure in support of the data including, but not limited to: providing physical security; backup and recovery processes; granting access privileges to system users as authorized by Data Trustees or their designees (usually the Data Stewards); and implementing and administering appropriate levels of controls over the information. The Office of Information Technology, Department of Public Safety, Development Office, and Sindecuse Health Center are examples of Data Custodians.
- **Data User:** individuals who need and use university data as part of their assigned duties or in fulfillment of assigned roles or functions within the university community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of that data. Any university employee with access to university data can be considered a data user.

Data classification is the responsibility of the Data Trustee in consultation with the Vice Provost for Academic Operations and Chief Information Officer.

Enforcement

Any person found to be in violation of this policy will be subject to appropriate disciplinary action as defined by current university policy or contract.

References

[Family Education Rights and Privacy Act \(FERPA\)](#)

[Human resources documentation](#)

[PPM Section 19 - Health Insurance Portability and Accountability Act \(HIPAA\)](#)

| Document Action | Group | Date |
|------------------------|---------------------------------------|-------------|
| Reviewed by: | WMU LAN Managers Group | 12-Aug-08 |
| Reviewed by: | OIT Leadership Team | 14-Aug-08 |
| Revised by: | Campus Information Security Committee | 03-Sept-08 |
| Revised by: | Campus Information Security Committee | 14-Jan-09 |