Bemidji State University Policies

Policy Name: University Data Governance and Security	**Effective Date:** 11/1/2020
Policy Owner: Chief Information Officer	**Last Review:** 10/14/2020
	Next Review: 9/1/2023

Policy Statement

This policy establishes University data governance roles, responsibilities, and standards to control data integrity, security, and quality in order to ensure greater accuracy, timeliness, and communication of data for decision-making.

Scope and Purpose of Policy

This policy is applicable to all institutional data collected, stored, transferred, or overseen by the University. This includes, but is not limited to, data in any form, including backup and archived data. The Chief Information Officer is authorized with the oversight of all University owned data handling and security of all data stored by the University.

This policy does not apply to faculty intellectual property. Nothing in this policy shall be interpreted to expand, diminish or alter academic freedom articulated under Minnesota State Board policy and system collective bargaining agreements.

The purpose of this policy is to establish data administration standards and ensure data integrity and security throughout the University. This policy seeks to establish consistent and well-defined data definitions across the University.

Definitions

University Data: Data collected, stored, reported, transferred, or overseen by the University. This comprises numbers, words, and images.

Data Ownership: University data is a University resource; individual units or departments may have stewardship responsibilities for portions of University data.

Data Dictionary: The University's official reference guide established by the Data Governance Work Group that documents the official University data definition for a data element referencing the original information source of a data element, the legacy or computation information of a data element, a narrative explanation of the data element, and where it is located.

Data Definition: The definition of a data element determined by the Data Governance Committee to be the University's official explanation and/or computation for a data element.

Data Storage Solution: A subject-oriented, integrated, time-variant and non-volatile collection of data in support of management's decision-making process.

Data Quality: The validity, accuracy, and relevancy of data.

Data Administration: The function of applying formal guidelines and tools to manage the University's information resource.

Security Administration: The function of specifying, implementing, and maintaining access control to ensure that only authorized individuals have access required to perform assigned duties or to fulfill University roles. Responsibility for security administration activities primarily falls under the governance of the Information Technology department.

System Administration: The function of maintaining and operating hardware and software platforms is termed System Administration. Responsibility for System Administration activities primarily falls under the governance of the Chief Information Officer.

Procedures

Data Governance Roles

- ***Data Governance Committee***: Responsible for the overall management of the University's data governance. This Committee will consist of Data Owners, Data Reporters, Data Custodians, and Data Users from administrative and academic units, including faculty, across the University.
- ***Data Owners***: An individual with authority and accountability for specified information (e.g., a specific business function) or type of institutional data. Included in this authority is the ability to grant and deny access to data or portions of institutional data under his or her authority. This individual shall assign responsibility to the appropriate data custodian(s) to ensure the protection of institutional data. The data owner is typically in a senior leadership position. There may be more than one data owner at a college, university, or the system office, depending on the authority and accountability for specified information (e.g., a specific business function) or type of institutional data.
- ***Data Custodians***: The data custodian is appointed by the data owner to assign the security classifications for institutional data and ensuring that the appropriate controls are implemented.
- ***Data Reporters***: Employees whose job responsibilities require them to access, manipulate, and analyze University data in order to provide official University reports and information to meet internal reporting requirements for decision-making and external reporting mandates.
- ***Data Users***: Individuals who access University data in order to perform their assigned duties or to fulfill their roles in the University community. Data Users are responsible for protecting their access privileges and for proper use of the University data accessed.

Quality and Integrity

- ***Data Definitions***: The Data Governance Committee will develop common University data definitions to ensure data consistency. Data Owners and Users will ensure appropriate procedures are followed to uphold and verify data quality and integrity.
- ***Institutional Data Storage***: Data Custodians will be responsible for the development of data storage, extraction, retention, and disposal. Data Owners will work with Data Custodians to develop appropriate archiving strategies and procedures.
- ***Data Reporting and Sharing***: The Data Governance Committee will be responsible for establishing data reporting standards, to include establishing appropriate census dates. Data Reporters will be responsible for identifying available reports, proper dissemination of reported University data and ensuring accuracy of compliance reporting.

Classification and Security

- ***Data Classification***: Data classifications will be established for University data based on Minnesota State Data Security Classifications as specified in System Procedure 5.23.2.
- ***Data Security:*** Appropriate data security roles and measures will be implemented for accessing data in order to protect the security and confidentiality of University data.

Rationale

This policy establishes data standards, data security, and identifies the shared responsibilities for ensuring that data in use throughout the University have integrity and effectively serves the needs of the University.

Supporting References

- Minnesota State Board Policy 5.22: Acceptable Use of Computers and Information Technology Resources https://www.minnstate.edu/board/policy/522.html
- Minnesota State Board Policy 5.23: Security and Privacy of Information Resources https://www.minnstate.edu/board/policy/523.html
- Minnesota State Board Procedure 5.23.2: Data Security Classification https://www.minnstate.edu/board/procedure/523p2.html