Data Governance Policy

Table of Contents

STATEMENT OF PURPOSE

College data are institutional assets maintained to support South Central College's central mission of providing accessible higher education to promote student growth and regional economic development. "College data" refers to collections of data elements relevant to the operations, planning, or management of any unit at SCC, or data that are reported or used in official administrative College reports.

To support effective and innovative management, College data must be accessible, must correctly represent the information intended, and must be easily integrated across SCC's information systems. The purpose of data governance is to develop College-wide policies and procedures that ensure that College data meet these criteria within and across SCC's administrative data systems.

Data governance at SCC is established at the direction of the College President. The purpose of the current Data Governance Policy is to achieve the following:

- Establish appropriate responsibility for the management of College data as an institutional asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Improve the security of the data, including confidentiality and protection from loss.
- Improve the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making.

The Data Governance Policy addresses data governance structure and includes policies on data access, data usage, and data integrity and integration.

ENTITIES AFFECTED BY THIS POLICY

Anyone at SCC who creates data, manages it, or relies on it for decision making and planning.

WHO SHOULD READ THIS POLICY

Data governance executive sponsors, data stewards, and all other SCC employees who use data, regardless of the form of storage or presentation.

POLICY STRUCTURE

1. Data Governance Structure
2. Data Access Policy
3. Data Usage Policy
4. Data Integrity and Integration Policy

POLICY

1. Data Governance Structure

Data Governance is the practice of making strategic and effective decisions regarding SCC's information assets. It assumes a philosophy of freedom of access to College data by all members of the community coupled with the responsibility to adhere to all policies and all legal constraints that govern that use.

In the interest of attaining effective data governance, the College applies formal guidelines to manage the College's information assets and assigns staff to implement them. While the College data custodian is assigned a leadership role and oversight for the activities of

data governance, this function is shared among the executive sponsors, data stewards, data custodians, and data users.

Executive sponsors will appoint data stewards, and through the establishment of data policies and institutional priorities, provide direction to them and data custodians. The College's data stewards comprise the Data Governance Council, a body that meets regularly to address a variety of data issues and concerns.

The following are general descriptions of the primary roles and responsibilities within Data Governance.

Executive Sponsors

Executive sponsors are senior College officials who have planning and policy responsibility and accountability for major administrative data systems (e.g., student, administrative, financial, and personnel) within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet institutional needs. Executive sponsors may include the following administrative personnel currently in place at SCC: Associate Vice President for Research and Institutional Effectiveness, Vice President for Student and Academic Affairs, Chief Financial Officer, Chief Information Officer, or the Chief Human Resources Officer. Executive sponsors meet as a group regularly to address a variety of data issues and concerns.

Director of Data Management

The director of data management works with the campus community to define a campus-wide structure of data stewardship by making explicit the roles and responsibilities associated with data management and compliance monitoring. This individual is responsible for coordinating data policies and procedures in the primary enterprise data systems – including

student, administrative, financial, and personnel – ensuring representation of the interests of data stewards, managers, and key users. The director of data management coordinates the meetings and agendas for the executive sponsors and Data Governance Council and provides support to related data management efforts. This individual is also responsible for developing a College culture that supports data governance in areas with critical peripheral databases that exist beyond the major administrative systems.

The director of data management works to ensure that all College data are represented within a single logical data model that will be the source for all physical data models. Informed by the Data Governance Council, the data administration area, led by the director of data management, is responsible for developing a College data model and corresponding data structures and domains.

The director of data management at SCC shall be the Associate Vice President for Research and Institutional Effectiveness, his/her designee, or the designee of the College President.

Data Stewards

Data stewards are appointed by executive sponsors to implement established data policies and general administrative data security policies. Data stewards, who comprise the Data Governance Council, are responsible for safeguarding data from unauthorized access and abuse through established procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support College data users. Included among data stewards are the following administrative personnel currently in place at SCC: Dean of Students, Director of Enrollment Management, Registrar, Director of Financial Aid, Assistant

Director of Human Resources, Database/Network Manager, Survey Researcher, and Academic Deans.

Data Custodians

Data custodians are College employees who most often report to data stewards and whose duties provide them with an intricate understanding of the data in their area. They work with the data stewards to establish procedures for the responsible management of data, including data entry and reporting. Some data custodians may work in a technology unit outside of the functional unit, but have responsibilities for implementing the decisions of the stewards. Technical data custodians may be responsible for implementing backup and retention plans, or ensuring proper performance of database software and hardware.

Examples of data custodians include information technology professionals, academic advisors, research office professionals, financial aid professionals, administrative assistants, department chairs, and business office professionals.

2. Data Access Policy

The purpose of the data access policy is to ensure that employees have appropriate access to institutional data and information. While recognizing the College's responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of College business. This policy applies to all College units and to all uses of institutional data, regardless of the offices or format in which the data reside.

Statement of Policy

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, and unnecessary restrictions to its access.

The College will protect its data assets through security measures that assure the proper use of the data when accessed. Access to protected data are granted by applying for operational data security access rights through the Minnesota State Colleges and Universities system office. Locally, data requests that include potentially sensitive or personally identifiable data by persons not typically allowed to view said protected data will be evaluated on a business need basis by the appropriate data stewards. Data/research requests made to the Office of Research and Institutional Effectiveness will use the established Machform for all requests, including a justifiable business need. Data access will be conducted in accordance with the policies established by the Executive Sponsors, the Director of Data Management, the Minnesota State Colleges and Universities Board of Trustees Policies and Procedures, and applicable state and federal statutes.

Any employee or non-employee denied access may appeal the denial to the Data Governance Executive Sponsors.

3. Data Usage Policy

The purpose of the data usage policy is to ensure that College data are not misused or abused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the data steward.

Statement of Policy

College personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update, read-only, and external dissemination.

Authority to update data shall be granted by the appropriate data steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the College's desire to provide excellent service to faculty, staff, students, and other constituents.

Read-only usage to administrative information will be provided to employees for the support of College business without unnecessary difficulties/restrictions.

Only those data elements designated as "directory information" (as defined by MnSCU policy or FERPA) can be externally disseminated for official or "nonofficial" reporting. Even release of directory information should be guided by the need to respect individual privacy and to protect the integrity of the data. The release of all other data must be approved by the responsible data steward.

Data usage shall be governed by applicable policies set out by local departments, the Office of Information Technology, the MnSCU system, and applicable federal and local laws.

Consequence of Noncompliance with Data Usage Policy

SCC employees and students who fail to comply with the data usage policy will be considered in violation of the relevant College codes of conduct and may be subject to disciplinary action or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data.

4. Data Integrity and Integration Policy

The purpose of this policy is to ensure that College data have a high degree of integrity and that key data elements can be integrated across functional units and electronic systems so

that College faculty, staff, and administration may rely on data for information and decision support.

Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element.

Data integration, or the ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Statement of Policy

College data will be consistently interpreted across all College systems according to the best practices agreed upon by the Data Governance Council, and it will have documented values in all SCC systems. Data administration will ensure that the needs of users of College data are taken into consideration in the development and modification of data structures, domains, and values. It is the responsibility of each data steward to ensure the correctness of the data values for the elements within their charge.

College data are defined as data that are maintained in support of a functional unit's operation and meet one or more of the following criteria:

1. the data elements are key fields, that is, integration of information requires the data element;
2. the College must ensure the integrity of the data to comply with internal and external administrative reporting requirements, including institutional planning efforts;
3. the data are reported on or used in official administrative College reports;
4. a broad cross section of users requires the data.

It is the responsibility of each data steward, in conjunction with the Data Governance Council, to determine which core data elements are part of College data.

Documentation (metadata) on each data element will be maintained within a College repository according to specifications provided by the Director of Data Management and informed by the Data Governance Council. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic calendar.

All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards, the Data Governance Council, or the Director of Data Management.

5. Section Reserved

This section is reserved for the addition of a data classification policy as set forth by the Office of Information Technology.

SEVERABILITY

If any provision of this policy or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this policy which can be given effect without the invalid provision or application, and to this end the provisions of this policy are severable.

RELATED DOCUMENTS & LINKS

- MnSCU Reporting and Data Services

  http://www.its.mnscu.edu/reportanddataservices/index.html
- The Family Educational Rights and Privacy Act (FERPA); 20 U.S.C. § 1232g; 34 CFR Part 99: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Health Insurance Information Portability and Accountability Act (HIPAA): http://www.hhs.gov/ocr/privacy/
- Minnesota Statutes, Chapter 13, Government Data Practices

  https://www.revisor.mn.gov/statutes/?id=13&view=chapter

CONTACTS

Director of Data Management

Associate Vice President for Research and Institutional Effectiveness

Chief Information Officer

DEFINITIONS

- Data Element – a single data item. For example, Year/Term is a data element.
- Data Value – the set of values that each data element can have. For example, 20151, 20153, and 20155 are values of the data element named building code.