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" are 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 Data Governance Policy is to achieve the following:

- Establish appropriate responsibility for the management of College data as an institutional asset.
- Ensure ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Ensure the security of the data, including confidentiality and protection from loss.
- Ensure the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making.
- Establish a record retention schedule and a clear delineation between what needs to be retained and what doesn't.

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

DATA Usage

Data usage shall be governed by all applicable federal, state and local laws, MinnState Board Policy, the Offices of Research & Institutional Effectiveness and Information Technology Services.

DEFINITIONS

- Data Element – a single data item. For example, YRTR (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 YRTR (year/term) code.
- Director of Data Management – Associate Vice President of Research & Institutional Effectiveness
- Data Governance Council – is comprised of Data Owners

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 custodians, 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
5. Record Retention

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 Director of Data Management is assigned a leadership role and oversight for the activities of data governance, this function is shared among the data owners, data custodians, and data users in accordance with the guidelines set forth within this document.

Data owners will appoint data custodians, and through the establishment of data policies and institutional priorities, provide direction to them and data users. The College's data owners 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.

Director of Data Management

The director of data management works with the campus community to define a campus-wide structure of data custodianship 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 custodians, managers, and key users. The director of data management coordinates the meetings and agendas for the 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 director of data management at South Central College shall be the Associate Vice President of Research and Institutional Effectiveness, his/her designee, or the designee of the College President.

Data Owners

Data owners are senior College officials and those appointed at the discretion of the president who has ultimate responsibility for data practices and compliance as South Central College. Data owners 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. Data Owners may include the following administrative personnel currently in place at South Central College: Associate Vice-President of Research and Institutional Effectiveness, Vice President of Student and Academic Affairs, Vice President for Finance and Operations, Vice President for Economic Development Chief Human Resources Officer, and the Dean of Student Affairs. Data Owners meet as a group regularly to address a variety of data issues and concerns and comprise the membership of the Data Governance Council.

"Data owners shall also maintain an inventory of private and confidential data sufficient to ensure compliance with Minn. Stat 13.025, subd 1. The Data owner shall ensure implementation of appropriate security controls and limit access to institutional data classified as highly restricted or restricted to those individuals who work responsibilities require access" System Procedure 5.23.2 Data Security Classification Part 4. Procedures--Subpart B.

Data Custodians

Data custodians are appointed by data owners to implement established data policies and general administrative data security policies and 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 custodians are the following administrative personnel currently in place at SCC: Dean of Student Affairs, Director of Admissions and

Financial Aid, Registrar, Director of IT Services, Academic Deans, members of the Office of Research & Institutional Effectiveness and Information Technology Services.

Data custodians are College employees who most often report to data owners and whose duties provide them with an intricate understanding of the data in their area. They work with the data owners to establish procedure(s) 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 owner.

Data custodians must use their operating instructions to determine the appropriate security controls to meet the information security requirements for the IT systems and data for which they are responsible. Technical data custodians may be responsible for implementing backup and retention plans, or ensuring proper performance of database software and hardware.

Data custodians are appointed by the data owners to assign the classification and ensure appropriate controls. The Data Custodian must document the classification of all data and re-review classifications every 3 years. Examples of data custodians include information technology, academic advisors, admissions, financial aid, human resource, payroll, administrative assistants, department chairs, members of the business office, and research office professionals.

Data users

All remaining South Central College employees are data users. Access to data and how that data may be accessed varies depending on the data user's role. If the data user has Common Alerting Protocol (CAP) server, Operational Data, Read-Eval-Print-Loop (REPL), or Enterprise Planning Management V11 (EPM11) privileges, then that access has been signed off by their immediate supervisor and the President. Data users with this level of access "shall access or use highly restricted data only for the business purposes that reasonably require and follow all applicable laws and Minnesota State policies, procedures and operating instructions related to data classification and access" System Procedure 5.23.2 Data Security Classification Part 4. Procedures--Subpart B.

Data users can access restricted and low-level information via South Central College's SharePoint where up-to-date decision-support dashboards are stored and maintained. The reports that are maintained via this password protected repository do not reveal data that would be classified as confidential and are designed in a manner that protects the confidentiality and privacy where appropriate.

2. Data Access Policy

The purpose of the data access policy is to ensure that employees have appropriate access to institutional data and information. 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 custodians. All requests made to the Office of Research and Institutional Effectiveness for data will require the use of the established MachForm, including a justifiable business need. Data access will be conducted in accordance with the policies established by the Minnesota State Colleges and Universities Board of Trustees Policies and Procedures, applicable state and federal statutes, and the Data Governance Council.In an effort to democratize data and increase the flow of information while maintaining an appropriate level of security and protecting sensitive information and privacy, the Office of Research & Institution Effectiveness has created several web-based reports hosted on SharePoint accessible only to South Central College employees. Information contained in these reports are not allowed to downloaded, nor is electronic access to a report allowed for external constituents. Access to these reports is typically granted upon request, however, any employee or non-employee denied access may appeal the denial to the Data Governance Council.

3. Data Usage Policy

The purpose of the data usage policy is to ensure that College data are not misused or abused, 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 custodian.

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 custodian 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.

Authority to disseminate information externally is restricted to the President, the Director of Data Management, Data Owners or their designees. Private or sensitive information, e.g., Social Security Numbers or Family Income Information should never be shared externally.

Directory Information

Only those data elements designated as "directory information" (as defined by MinnState policy or FERPA) can be externally disseminated for official or "nonofficial" reporting. Directory Information is information contained within a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. FERPA requires each institution to define its directory items—see the Directory Information Website. The release of directory information should be guided by the need to respect individual privacy and to protect the integrity of the data. Limited Directory Information is a category of data that allows as school to specify a subset of Directory Information that can only be released to specific parties and/or for specific purposes. The release of all other data must be approved by the responsible data custodian. Directory and Limited Directory Information are denoted on South Central's Directory Information Website.

Student email addresses and Star ID numbers are defined as Limited Directory Data for enterprise technology related purposes internal to the Minnesota State Colleges and Universities system that are approved by System Office IT, including, but not limited to, inclusion of email addresses and Star ID numbers in a directory accessible to Minnesota State students and employees.

At South Central College, students are individuals who currently or formerly enrolled or registered, applicants for enrollment, or individuals who receive shared time educational services from South Central College. All students at South Central College have the same rights regarding their educational data regardless of age.

Non-Directory Information

All information not directly listed in the link above are classified as non-directory information or not public data--System Procedure 5.23.2 Data Security Classification Part 3. Definitions. Chief among non-directory information are Educational Records and data in any form directly relating to an individual or group of students maintained by South Central College or by a person acting for South Central College.

These data includes but are not limited to

a. Admissions materials,
b. Financial aid records,
c. Transcripts,
d. Class lists,
e. Class schedules,
f. Grades,
g. Graded exams or papers,
h. Records of disciplinary proceedings,
i. Photographs,
j. Work study records
k. Most personal Data
l. Donor contact Information
m. ID numbers if not directory data

The information contained in a students' education record shall never be shared or considered "directory information" without the express written permission of the student. Additional examples of this type of information are:

a. Financial records of the student's parents or guardian;
b. Confidential letters or statements of recommendation placed in education records before January 1, 1975, or after January 1, 1975, if the student waived right of access;
c. Records of instructional personnel that are kept in the sole possession of the maker and are not accessible or revealed to any other individual except a temporary substitute for the maker and are destroyed at the end of the school year;
d. Records of law enforcement units (if law enforcement unit is a separate entity and the records are maintained exclusively by and for law enforcement purposes);
e. Employment records related exclusively to a student's employment capacity (not employment related to status as a student, such as work study) and not available for use for any other purpose;
f. Organizational memberships
g. Work retained for assessment purposes (need to re-word this one)
h. Medical and psychological treatment records that are maintained solely by the treating professional for treatment purposes;
i. Records that only contain information about a student after that individual is no longer a student at the institution (alumni data).
j. Social Security Numbers.
k. Credit Card or other payment Card numbers.
l. Security or access codes and passwords.
m. Personal Health Information.
n. Non-public investigation data.
o. IT Credentials for systems that manage restricted data
p. Biometric data.
q. Trade secrets data or other intellectual property protected by a non-disclosure agreement.

Annual Notification

Students are informed of their rights under federal and state privacy laws through an annual notice of rights and this policy. This notification will include a link for students to request the college withhold their directory information.

Access to Students Records

Subpart A: Public student data (i.e. directory information) may be available upon request to all parties, However, South Central College reserves the right to refuse, modify or limit the amount of directory information released to requestors as our guiding principles are the need to respect individual privacy and to protect the integrity of the data.

Subpart B: Students have the right of access to their own private education records and to challenge the accuracy of the information contained therein. They have the right to authorize the release of any private education records to a third party. Parents are considered a third party regardless of the student's age, dependent status, or enrollment category. However, a school may disclose information from an "eligible student's" education records to the parents of the student, without the student's consent, if the student is a dependent for tax purposes (FERPA Policy FAQ #6).

Subpart C: School officials with legitimate educational interest have the right of access to student education records.

Subpart D: Other circumstances authorize the college to release education records to a third party without the student's written consent.

Consequence of Noncompliance with Data Usage Policy

South Central College 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 custodian to ensure the correctness of the data values for the elements within their charge. It is the responsibility of data custodians to maintain definitional integrity of elements and fields, assure that the entry of data into the various systems by either themselves or data custodians is completed in a timely manner and that definitions—and definitional changes—updates to fields, and operational (data entry) modification are communicated clearly and in a timely manner with the Director of Data Management.

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 custodian, 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 custodians, the Data Governance Council, or the Director of Data Management.

5. Record Retention Policy

The purpose of this policy is to ensure that College records are effectively managed and that to establish a schedule which sets out the periods of time for which an organization's business records are to be retained. A record retention schedule protects both the college interests and the public's rights by providing guidance to the college about the management of records.

Statement of Policy

Minnesota State Colleges and Universities are subject to the state's records management statue, Minn. Stat. Sect. 138.17, and the official records law, at Minn. Stat. 15.17. These laws, in general, provide directives concerning the retention and destruction of "official records," i.e., records that are necessary to a full and accurate knowledge of official activities. Government entities are supposed to have data retention schedules for the official records that they keep; those schedules must be approved by a statewide records disposition panel headed by the Department of Administration. Official records are to be retained in accordance with that schedule, and of particular importance, official records may not be destroyed unless pursuant to an approved schedule.

Minnesota's Official Records Act (Minnesota Statutes Sect.15.17) requires government entities to "make and preserve records necessary to a full and accurate knowledge of their official activities."

A retention schedule informs faculty, staff and administrators of the minimum length of time to keep certain records and gives the college authority to destroy records when appropriate. It specifies how long records must be kept and includes references to laws that govern the retention period for particular documents. College personnel should follow their college's record retention schedule regarding the destruction and retention of all records collected, created, received, maintained, or disseminated by a college. South Central College's Record Retention Schedule follows the guidelines established by the Minnesota Historical Society. The Record Retention Schedule is housed as an excel spreadsheet and PowerBI report on the Office of Research and Institutional Effectiveness' SharePoint Site. Here you can also find HR Records Retention Schedule and Minn. State System Office Records Retention Schedule.

6. Data Classification

The purpose of this policy is to support the classification of data to allow for the protection of data that is created, stored or transmitted by South Central College's data, in terms of confidentiality, integrity, and availability.

Statement of Policy

In relation to System Procedure 5.23.2 Data Security Classification Part 4. Procedures this section provides additional guidance for classifying and protecting South Central College's information resources. It outlines the security objectives in the left column and assesses the potential impact to South Central College (SCC) should certain events occur which jeopardize the information and information systems needed by the College to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The three levels of potential impact on SCC or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) are as follows:

The potential impact is LOW if: − The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on SCC's operations, assets, or on individuals.

The potential impact is Restrcted if: − The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on SCC's operations, assets, or on individuals.

The potential impact is Highly Restricted if − The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on SCC's operations, assets, or on individuals.

Public information, i.e. information that can be communicated without restrictions, and is intended for general public use, is not included in the framework below as this data will not cause harm to any individual, group, or to SCC if made public. Examples include: Standard guidelines and policies; Published College Strategy; Contact details; maps; Course catalogue, public web page, press releases, event details, advertisements and directory information.

Potential Impact			
Security Objective	**Low**	**Restricted**	**High Restricted**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on SCC's operations, assets, or on individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on SCC's operations, assets, or on individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on SCC's operations, assets, or on individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on SCC's operations, assets, or on individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on SCC's operations, assets, or on individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on SCC's operations, assets, or on individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on SCC's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on SCC's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on SCC's operations, assets, or on individuals.

Potential Impact			
Security Objective	**Low**	**Moderate**	**High**
Data Classification	**SCC Controlled** With this classification protection of information is at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to SCC. Examples: Meeting minutes; unit working & draft documents.	**SCC Restricted** SCC has a legal, regulatory or contractual obligation to protect the information with this classification. Disclosure or loss of availability or integrity could cause harm to the reputation of SCC, or may have short term financial impact on the college. Examples: Student or employee records; grades; employee performance reviews; personally identifiable information.	**SCC Highly Restricted** Protection of information is required by law or regulatory instrument. The information within this classification is subject to strictly limited distribution within and outside the College. Disclosure would cause exceptional or long term damage to the reputation of SCC, or risk to those whose information is disclosed, or may have serious or long term negative financial impact on the College. Examples: Physical or mental health record relating to individuals; Critical research data

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

- Minnesota State Reporting and Data Services
- The Family Educational Rights and Privacy Act (FERPA); 20 U.S.C. § 1232g; 34 CFR Part 99
- Health Insurance Information Portability & Accountability Act (HIPAA)
- 2017 Minnesota Statutes: Chapter 13-Government Data Practices
- SCC Data Glossary
- SCC Query Encyclopedia

CONTACTS

Associate Vice President of Research and Institutional Effectiveness

-