Policy #230
Date Approved: 5/29/2024
Date Amended:
Responsible Office: Cabinet

SUBJECT: DATA GOVERNANCE POLICY

1.0 PURPOSE

1.1. This policy outlines the structure of Data Governance at Snow College by defining Data Governance and Data Management, placing ownership of Data Governance in the Cabinet and Data Management with the Director of Analytics and Institutional Research; and defining data as an asset that should be cultivated and used to fulfill the College's mission and improve student success.

1.2. This policy applies to all Snow College students, faculty, staff, student workers, contract employees, temporary employees, consultants, contractors, vendors, and third-party agents of the College. As of the date of this policy, the College recognizes Oracle as its central database and Banner as its central Enterprise Resource Planning (ERP) system, and covers all institutional data, whether individually controlled, shared, standalone, or networked. The officially recognized central database and central ERP system used by the College are considered the authoritative sources of truth for the College. This policy applies to all types of physical or electronic data transmission and all other types of data collected for college business purposes including data collected for research purposes.

2.0 DEFINITIONS

2.1. *Analytics and Institutional Research (AIR):* The AIR office is the central source of data and statistics related to the College. It helps define business processes that maintain and enhance data integrity. AIR is responsible for managing data governance at the College; providing proactive analytical resources; validating data; identifying and remedying data integrity issues; and providing reliable, consistent, and operational reports and dashboards to the College.

2.2. *Data Coordination Group (DCG):* An advisory committee composed of the Director of AIR, the College's Data Stewards, and those Cabinet appoints to the committee. The DCG exists to coordinate the development, use, dissemination, and management of the College's data, and for coordinating compliance with the College's Data Governance Plan.

2.3. *Data Custodians*: Employees who have delegated operational responsibility over information assets or data systems, and access/permissions to those systems delegated to them by a Data Steward. In many cases, there will be multiple Data Custodians within a functional area overseen by the Data Steward. An enterprise application may have teams of Data Custodians, each responsible for varying functions.

2.4. *Data Governance:* Data Governance is the structure, strategies, and supports that ensure institutional data is seen, managed, protected, and used as a strategic College asset. Data Governance facilitates accurate analytics and reporting, which helps answer key questions and inform decision-making by leadership, internal audiences, and external agencies.

2.5. *Data Governance Plan (Plan):* Snow College's comprehensive Data Governance Plan that ensures College data will be protected according to College, Utah's System of Higher Education, federal, state, and other jurisdictional or industrial (e.g. GDPR, PCI) guidelines/regulations against deliberate, unintentional, or unauthorized alteration, destruction, or disclosure. The Plan also establishes data standards and roles and responsibilities for data management at the College. The Plan has two functions:

2.5.1. Complying with Utah's laws for managing education data[1] in that it

2.5.1.1. Incorporates reasonable data industry best practices to maintain and protect student data and other education-related data;

2.5.1.2. Describes the role, responsibility, and authority of the College's privacy officer;

2.5.1.3. Provides necessary technical assistance, training, support and auditing;

2.5.1.4. Describes the process for sharing student data between the educational entity and another person;

2.5.1.5. Describes the education entity's data expungement process, including how to respond to requests for expungement;

2.5.1.6. Describes the data breach response process; and

2.5.1.7. It is published annually and available on the institution's website or the Utah System of Higher Education's website.

2.5.2. Operationalizing Data Governance at Snow College by

2.5.2.1. Establishing data standards; and

2.5.2.2. Outlining the roles and responsibilities of those who in any way handle institutional data.

2.6. *Data Lineage.* Documentation showing the point of origination for all data points as well as any transformations that have been applied to the data. It gives visibility to where the data has been, allows it to be reproduced, and greatly simplifies the process of tracing errors back to the root cause.

[1] Higher Education Data Privacy and Governance Revisions (S.B. 226, 2022 Gen. Sess. (Ut. 2022)) (lines 155-168).

2.7. *Data Management*. The oversight and development of the policies, practices, processes, and structures that develop, create, store, secure, process, retrieve, analyze, and disseminate data.

2.8. *Data Options*. Data Options are the standardized values available in fields in data systems such as Banner. In Banner, for example, these are often held in "validation tables."

2.9. *Data Standards.* The College's principles and practices for managing data at Snow College. Data Standards are the principles by which data, reports, data-generating processes, and data systems are developed, managed, created, and maintained. Data Standards include:

2.9.1. *Data Accuracy*. Data must be correct, appropriate to the request or question pursued, and represent the characteristics intended to be conveyed.

2.9.2. *Data Analysis*. Data provided must result from using the appropriate analytical tools and techniques for reaching appropriate informed, data-based conclusions and decisions. This includes the development of a college-wide data glossary.

2.9.3. *Data as an Asset*. Data is an Asset vital to informed decision-making and student success. As an asset, data is only as valuable as the processes that create and maintain them. It is valuable if it is accurate, high in quality and integrity, and integrated across all data repositories.

2.9.4. *Data Flexibility*. Data systems should be flexible enough to change with the needs of the institution and the success of students without violating the integrity and usefulness in the analysis conducted for decision-making.

2.9.5. *Data Integration*. Data Integration is the connection or ability to connect the various data sources that hold Snow College data. All institutional data must be able to be integrated and/or affiliated with Snow College's ERP.

2.9.6. *Data Integrity*. Data Integrity results from the consistency of data over time. To the extent possible, data values within the data system should have the same meaning over time so analysis, especially predictive analysis, is possible.

2.9.7. *Data Privacy*. Data about individuals is private and to be held, disseminated, and used under strict adherence to the principles, policies, and laws governing the privacy of data.

2.9.8. *Data Quality*. Report data needs to meet the highest standards of accuracy, usability, and accessibility. This includes preventing

unnecessary duplication, deleting, and updating of data within data systems.

2.10. *Data Steward*: An individual who has been designated as accountable for a specific functional area within a system that stores, transmits, or uses College data. Data Stewards are the administrators responsible for operations that handle institutional data storage, creation, and processing. Data Stewards are responsible for the functional area and any data systems attached or otherwise integrated with the functional area's data. Data Stewards have the authority for data in their respective area, but must collaborate and coordinate with the DCG before making procedural changes to data processes, whenever possible.

2.11. *Data Technician.* Employee(s) in the Information Technology Office appointed to liaison with the DCG on data systems management.

2.12. *Director of Analytics and Institutional Research (Director).* Director of AIR and chair of the DCG. The director has operational and coordinating responsibilities of Data Governance at Snow College.

2.13. *Enterprise Resource Planning (ERP) System*. The College's primary integrated data and resource computer system for managing and coordinating the College's operations.

2.14. *Functional Areas*. Discrete, though interconnected, areas defined within the ERP that function to create, store, and/or process related education data. These areas include but are not limited to the following: (a) Banner Student, (b) Banner Financial Aid, (c) Banner Admissions, (d) Banner Human Resources, (e) Banner Alumni, (f) Banner Finance, (g) Banner General, and (h) Learning Management Software (LMS). Functional areas include the data systems connected to the ERP.

2.15. *Institutional Data*. All data relevant to operations, unit-level planning and management, data used or reported in official College reports, and data that resides in or is generated from enterprise transactional systems. Institutional Data includes education data.

2.16. *Report Writers*. College personnel who are responsible for gathering or analyzing raw data for production in understandable, usable mediums such as reports and dashboards. Report writers also create ad hoc reports to answer questions posed that require aggregating data.

3.0 POLICY

3.1. Data is an institutional asset.

3.1.1. Data is vital to the College fulfilling its mission, improving the success of students, and empowering College employees. Thus, data will be managed (created, identified, defined, developed, and maintained)

with controls established to manage data completeness and validity and reduce data redundancy, alteration, and destruction. Data is created and maintained to fulfill the College's reporting and record-keeping responsibilities.

3.1.2. Institutional Data is owned by the institution. While departments and other units within the College have operational-level responsibility for subsets of Institutional Data, no single person, department, or unit within the institution "owns" any Institutional Data.

3.2. Data Governance at Snow College is owned by the Cabinet with Data Management delegated to the Director of AIR. However, Data Governance is a shared effort by which data is created, identified, defined, developed, used, and maintained.

3.3. The Director of Analytics and Institutional Research will

3.3.1. Serve as the chair of the DCG;

3.3.2. Develop an operational Data Governance strategy with the direction of Cabinet that adheres to Data Standards;

3.3.3. Develop a Data Governance Plan in coordination with Cabinet, the DCG, and the Offices of Information Security and Information Technology;

3.3.4. Define business processes that promote, maintain, and enhance Data Integrity;

3.3.5. Work with the College's Report Writers to ensure official reports and data submissions are timely, accurate, and complete, and not disrupted by changes within the College's ERP and supporting systems;

3.3.6. Manage a data warehouse in coordination with the Office of Information Technology that will act as a repository for report data and of reported data;

3.3.7. Create, in coordination with DCG members, a repository for documenting Data Lineage to improve data understanding and usage, as well as for documenting data definitions that also include how and where data is stored and where it is used;

3.3.8. Coordinates activities with all data stewards responsible for validation tables in the College's ERP (Banner); and

3.3.9. Create bylaws for the DCG that explicate the roles and responsibilities of DCG members that at least incorporate those articulated in Appendix I.

3.4. Data Coordination Group. To ensure data and reports adhere to the Data Standards, the DCG coordinates the creation, identification, definition, development, and maintenance of data at Snow College under the direction of the Director.

3.4.1. The DCG is responsible for coordinating the use of the College's ERP and associated systems in compliance with the Data Standards, establishing project plans for approved proposals, and meeting the objectives of the Data Governance Plan. Within their own area of leadership, members will assist in documenting, identifying and executing necessary process improvements, creating metadata documentation, verifying curated data sources, and creating processes for data quality assurance (e.g. missing data, data consistency).

3.4.2. The Data Coordination Group is composed of the following:

3.4.2.1. Director of AIR;

3.4.2.2. Data Stewards; and

3.4.2.3. Others as designated by the Cabinet.

3.4.3. The DCG focuses on six (6) areas: (a) data policies and standards, (b) data quality, (c) data architecture, (d) privacy compliance, (e) establishing standardized, transparent, and documented processes, and (f) proposing resolutions to data integrity issues and conflicts.

3.4.4. The DCG also has the following responsibilities:

3.4.4.1. Ensuring data is treated as a college asset.

3.4.4.2. Helping develop and enforce the Data Governance Plan.

3.4.4.3. Implementing Data Standards.

3.4.4.4. Implementing and maintaining a data glossary.

3.4.4.5. Identifying and publishing a list of data stewards and custodians and the areas they administer and manage.

3.4.4.6. Reviewing proposals to modify the College's ERP and supporting systems.

3.4.5. The Data Coordination Group may create subcommittees for the effective and efficient completion of its responsibilities.

3.5. Data Stewards must collaborate and coordinate with the DCG before making procedural changes to data processes.

3.5.1. Data Stewards may delegate operational responsibilities for parts of their functional areas to Data Custodians. Data Stewards will ensure the list of Data Custodians compiled by the DCG is accurate.

3.6. In the event that collaboration and coordination for a procedural change cannot be achieved due to disagreements within the DCG, the Cabinet will act as the final decision maker on how to proceed.

4.0 REFERENCES

4.1. Snow College Information Technology Acceptable Use Policy (Policy #225)

4.2. Snow College Data Classification and Handling (Policy #226)

4.3. Snow College Information Security (Policy #227)

4.4. Snow College Risk Management

4.5. Utah Senate Bill 226: Higher Education Data Privacy and Governance Revisions (S.B. 226, 2022 Gen. Sess. (Ut. 2022))

4.6. Utah Code § 63G-2 Government Records Access and Management Act (GRAMA) (Ut. Code Anno. § 63G-2)

4.7. Utah State Board of Higher Education Policy R345 Information Technology Resource Security

APPENDIX I: ROLES AND RESPONSIBILITIES

Director of AIR

1. Coordinates with the Information Security Office and other integral parties the creation and maintenance of the College's Data Governance Plan.
2. Coordinates the improvement of business processes according to Data Standards.

Report Writers

1. Adhere to Data Standards and the Data Governance Plan.
2. Standardize reports by using the data repository and warehouse.
3. Adhering to policies, guidelines, and procedures pertaining to the protection of Institutional Data.
4. Help build and maintain an accurate, accessible, and understandable data glossary.
5. Help build the data repository/warehouse that includes the means of tracking Data Lineage.

Data Stewards

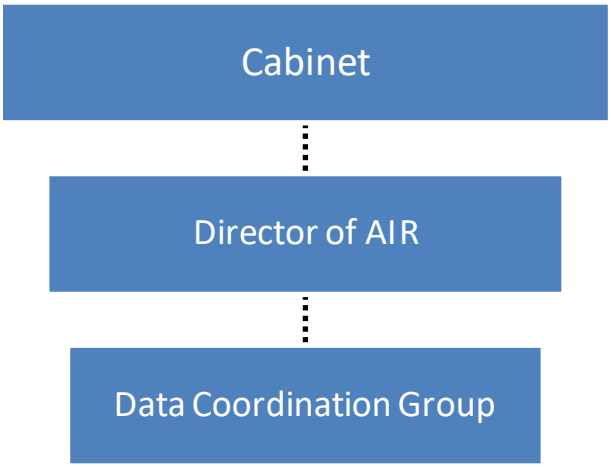
1. Assign an appropriate classification to Institutional Data. All Institutional Data should be classified based on its sensitivity, value, and criticality to the College. See Snow College Data Classification and Handling Policy, #226.
2. May assign day-to-day administrative and operational responsibilities for Institutional Data to one or more Data Custodians.
3. Determine the appropriate criteria for obtaining access to Institutional Data and conduct an annual review of data access. Provision and deprovision access to Institutional Data.
4. Approve standards and procedures related to day-to-day administrative and operational management of Institutional Data.
5. Document and disseminate administrative and operational procedures to ensure consistent storage, processing, and transmission of Institutional Data.
6. Implement appropriate safeguards for proper page and field usage in Snow College's ERP system (Banner). Data Stewards are responsible for proposing changes in the use of the ERP, to include new and changed usages of the ERP's pages and fields. Data Stewards should ensure that these changes promote storing data in the ERP that Ellucian sanctions and configuring the ERP in a way that does not adversely impact other processes of the ERP system. Also, if institutionally feasible, Data Stewards may propose altering current usages to align with the ERP's design and purpose.
7. Implement reasonable and appropriate physical and technical security controls to protect the confidentiality, integrity, and availability of Institutional Data in coordination with the Information Security Office.
8. Understand and approve how Institutional Data is stored, processed, and transmitted by the College and by third-party Agents of the College.
9. Define risk tolerance and accept or reject risk related to security threats that impact the confidentiality, integrity, and availability of Institutional Data. Information security requires a balance between security, usability, and available resources. Risk management plays a significant role in establishing this balance. Understanding what classifications of data are

being stored, processed, and transmitted will allow Data Stewards to better assess risks. Understand legal obligations and the cost of non-compliance will also play a role in this decision-making. Both the Information Security Office and the College's general counsel can assist Data Stewards in understanding risks and weighing options related to data protection.

10. Understand how Institutional Data is governed by Institutional policies, state and federal regulations, contracts, and other legally binding agreements. For example, Data Stewards are responsible for having a general understanding of legal and contractual obligations surrounding Institutional Data under the Family Educational Rights and Privacy Act ("FERPA").
11. Report actual or suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to the Director of AIR or the Information Security Office.

APPENDIX II: Data Governance Structure

Data Governance Structure



College Organizational Structure