SDSU Data Governance Guidelines[1]

Lucid Chart

I. Background

Several strategic working groups, SDSU's 2015 WASC reaccreditation self-study, and the IT Governance Council have all recommended implementing a data governance structure. The recommendations recognize that institutional data are the foundation for sound decision-making and are fundamental for effectively leveraging artificial intelligence capabilities. These data are critical strategic assets of the University, and thus require appropriate governance structure for the collection, management, security and use of data. As these data are regularly collected, maintained, and shared by many units on campus, this document seeks to outline a clear, consistent, and sustainable approach to data governance in order to protect the integrity, security, and proper use of University data.

The following guidelines supplement, operationalize and shall not conflict with Federal, State, CSU and campus policies and laws that govern the use of personally identifiable information. These include CSU Information & Security Policy, NIST data privacy standards, SDSU Information Security Office policies and SDSU's University Senate policies and other campus policies.

[1] The document referenced similar policies/guidelines from CSU-Fullerton which referenced the UC-Davis, CSU-San Marcos, University of North Carolina, Australian Catholic University, University of New South Wales.

II. Purpose

The Data Governance Guidelines are intended to:

1. Define the roles and responsibilities for data collection, access, storage, security, and destruction, and to establish clear lines of accountability.
2. Develop and regularly assess best practices for data management, access control, and security.
3. Establish a mechanism for granting data access and managing usage requests.
4. Define the roles and responsibilities for maintaining institutional metadata which define what data mean and help users understand the appropriate use of data.
5. Establish and empower the Data Governance Technical Committee to establish standards and/or procedures for accessing, retrieving, reporting, managing, and storing data.

III. Scope

The Data Governance Guidelines establish the framework of standards and guidelines to be followed in the management of institutional data, including procedures that govern the creation of data architectures and access mechanisms.

This document applies to all institutional data collected or used in the operations of the University including Global Campus and all of its auxiliary enterprises (e.g. SDSURF, Aztec Shops). The scope covers (though not limited to) institutional data in any form, including print, electronic, audio visual, backup, and archived data. Examples of institutional data include (though are not limited to) metrics, measurements, logs, demographic information, identity information, performance, assessment and evaluation information, records of professional, curricular or co-curricular activities, etc. Those data collected by campus stakeholders in the course of research and creative activities are <u>not included</u> under the guidelines <u>only if</u> those data are unrelated SDSU students, faculty, or staff, or to SDSU as an institution.

These guidelines are intended to set standards for securing and providing access to data and shall not conflict with policies and procedures established in SDSU's University Senate policies.

IV. Principles

The following set of principles underlie the SDSU Data Governance Guidelines:

1. **Alignment with University mission:**
    a. Institutional data support the mission of the University, facilitates evidence-based decision-making, and aims at continuous improvement;
    b. Personal use of institutional data is prohibited;
    c. Use of data that deviates from the University's policies, including diversity, equity, and inclusion, is also prohibited.
2. **Transparent guidelines:**
    a. Policies, procedures and documentation regarding institutional data should be clear, transparent, consistently applied, and implementable.

3. **Sound practices:**
    a. Sound record management practices (e.g., records retention, destruction) should be applied to both institutional data and unofficial University records;
    b. The systems for institutional data should be well-defined and kept current;
    c. Unnecessary duplication of institutional data should be discouraged;
    d. Outdated or data no longer in need should be securely destructed;
    e. All data-related practices should be documented in an auditable and traceable manner.
4. **Legitimate purposes:**
    a. Data should be accessed and shared appropriately only when there is a legitimate business purpose.
5. **Data security:**
    a. Data security measures should be in place at all times to ensure the safety, quality, and integrity of University data of all formats (paper, digital, audio/visual, etc.).
    b. Data should be stored in a secure manner appropriate for the corresponding data formats, and accessible only by authorized users.
6. **Data privacy:**
    a. Data containing information about individuals should be treated with respect, and follow appropriate data privacy and security protocols.
7. **Data validation:**
    a. Data used or shared inside or outside the University should be validated at multiple levels (e.g., by the Data Stewards, Data Experts) to ensure the quality, integrity and security of data are not compromised.
8. **Data semantics:**
    a. Data definitions should be kept current and in a centralized catalog, accessible to campus personnel to promote consistent use of data, shared vocabulary and cross-functional collaboration.
9. **User training:**
    a. Any individuals involved in the handling of institutional data must be properly trained in the relevant regulations and practices (e.g., CSU SumTotal Course: Data Security Introduction and FERPA). This includes individuals conducting sponsored research.

V. Roles and Responsibilities

The University owns all institutional data. These data are not owned by any one person, department, unit, or division. However, responsibilities for specific aspects of data management and security are held by individuals within certain roles and groups within the University. The roles and responsibilities outlined below will govern institutional data management, access, accountability, and security.

1. **Executive Leadership**. SDSU's Executive Leadership are the final decision-makers related to data governance. This includes the University President, Council of Vice-Presidents (COVP) and IT Governance Council (ITGC).

Data Type	*Exec Leadership*
All	CIO
	ITGC
	President
Budget & Financial	VP BFA
	VP DRI
Development & Alumni	VP URAD
Employee	VP BFA
Faculty records	Provost
HIPAA	VP SACD
Student records	Provost
	VP BFA
	VP SACD

2. **Data Governance Technical Committee (DGTC)**

The Data Governance Technical Committee is responsible for the oversight of appropriate data processes in support of data-informed decision-making at SDSU. DGTC is charged with developing and updating the campus guidelines regarding data use. In the absence of Federal, State, and CSU policy, DGTC is the governing body to make recommendations about University data policies.

Specifically, DGTC:

- Identifies opportunities for more strategic use of data necessary to achieve University goals;
- Develops, regularly reviews, and updates as appropriate campus guidelines related to data use;
- Monitors existing data governance structure to ensure appropriate groups and units are charged with tasks appropriate for their expertise or interest;
- Provides oversight on (but not limited to) access to and use of data. Reviews and approves complex or controversial data access requests.

DGTC is composed of representatives from University divisions and units who have knowledge of institutional data and best practices in the use of such data. Each DGTC representative is responsible for bi-directional communication within their division communicating guidelines to their data trustees and bringing relevant issues back to DGTC. The membership of the DGTC is appointed by the President, and is reviewed and renewed annually:

Division	Dept	Name	Count
− Acad Affairs	− ASIR	Cris Manlangit	1
		Jeanne Stronach	1
	− Education	Sandra Kahn	1
	− Engineering	Yusuf Ozturk	1
	− Enr Svcs	Stefan Hyman	1
	− Global Campus	Meng Phuong	1
	− Grad Std	Andrew Bohonak	1
	− IV	Henry Villegas	1
	− Provost Office	Sonja Pruitt-Lord	1
	− Sciences	Stephen Schellenberg	1
Acad Affairs Total			10
− BFA	− Fin Ops	Beth Warrem	1
		Crystal Little	1
	− HR	Heidi Poon	1
BFA Total			3
− Faculty	− Math & Stats	Richard Levine	1
	− MIS	David Goldberg	1
Faculty Total			2
− IT	− CIO	James Frazee	1
	− COO	Sean Hauze	1
	− ERP	Cyndie Winrow	1
		Kristina Moller	1
IT Total			4
− SACD	− Admin	Randall Timm	1
	− Career Svcs	Jesus Jimenez	1
	− Financial Aid	William Pierce	1
	− PECA	Maureen Guarcello	1
SACD Total			4
− URAD	− Alumni	Jeffrey Luko	1
URAD Total			1
Grand Total			**24**

DGTC is charged by and reports to SDSU Executive Leadership including the President, COVP and the IT Governance Council, who make final decisions. The DGTC will meet quarterly, with the possibility of more frequent meetings as needed.

3. **Data Trustees** *(see SDSU Data Sources, Update 2025)*

Data Trustees are members of the senior administration who are accountable for the planning and decision-making related to SDSU's institutional data and oversee units responsible for the collection, generation, management, and dissemination of institutional data. Specifically, they include:

Data Type	*Division*	*Trustee*
All	IT	AVP ERP
		ITSO
Budget & Financial	BFA	
		Athletics
		AVP Bus Ops
		AVP Fin Ops
		AVP Public Safety
		Sr AVP Admin
	DRI	VP DRI
Development & Alumni	URAD	
		AVP Development
		Exec Dir Alumni
Employee	BFA	Sr AVP Admin
Faculty records	Acad Aff	AVP ASIR
		AVP RM
HIPAA	SACD	Sr AVP
Student records	Acad Aff	Assoc Dean-CGS
		AVP ASIR
		AVP EM
		AVP FASS
		Sr AVP
		AVP Intl Affairs
		Dean CAL
		Dean Education
		Dean GC
	BFA	Athletics
		Exec Dir A.S.
	SACD	AVP
		Sr AVP

Sponsored research data is not covered under SDSU's Data Governance Guidelines.

4. **Data Stewards** *(see SDSU Data Sources, Update 2025)*

Data Stewards are individuals designated by Data Trustees to be responsible for the day-to-day management of institutional data and access to the data of particular organizational units. Data Stewards are responsible for implementing both campus-wide and unit-specific data governance guidelines. Specifically, the Data Stewards manage access to data for employees within their units by(1) authorizing the request of data access based on the employees' roles, (2) ensuring the employees receive proper training, and (3) monitoring whether the employees successfully and appropriately execute their data access and roles and delete data per guidelines. Specifically, Data Stewards include:

Division	Data Type	Steward
Acad Aff	Faculty records	ASIR
		AVP RM
		College of Education
	Student records	Admissions
		Advising
		ASIR
		CGS
		College of Education
		GC Registrar
		Global Campus
		ISC
		Registrar
		SSRL
BFA	Budget & Financial	Athletics
		Controller
		Facilities
		Housing
		HR
		Logistical Svcs
		Parking
	Employee	HR
	Student records	A.S.
		Athletics
DRI	Budget & Financial	Foundation
	Sponsored Research	N/A
IT	All	ERP FA
		ITSO
SACD	HIPAA	Student Health Services
	Student records	Career Svcs
		Disability Services
		ECRT
		EOP
		NPP
		OFAS
		Ombuds
		PECA
		Student Life
		Test Office
URAD	Development & Alumni	Alumni
		Development

5. **Data Experts**

Data Experts are individuals within units designated by Data Trustee and/or Data Steward to have direct physical control over physical or electronic information systems that house institutional data. Data Experts have operational responsibilities in assisting Data Stewards with day-to-day data related activities, including (though not limited to) collecting, generating, managing, maintaining, defining, distributing, securing, and disposing of institutional data. Data Experts have high level knowledge and expertise in the content of data or information systems within their responsible areas. Such level of knowledge and expertise enables Data Experts to serve in the risk management capacity for their units, regularly accessing risk related to data access and use, creating and implementing data management procedures, documenting data definitions, and maintaining procedures for the secure disposal of University data.

6. **Data Users**

Data Users are individuals – either employed by or affiliated with the University – that have been granted authorization by Data Trustees to access institutional data to carry out day-to-day responsibilities. Data Users are not involved in the data governance process, but are expected to comply with the University data governance guidelines. As such, they should complete proper training to ensure a proper understanding of relevant policies and procedures. Data users must acquire data through proper channels, store and handle data in secure manners, safeguard the access to identifiable data to authorized individuals and dispose of data per guidelines.

VI. Data Access

SDSU regularly provides aggregated data about our students, faculty, and staff. Multiple public dashboards are available via the Analytic Studies & Institutional Research (ASIR). Additional and more disaggregated data are available to SDSU faculty and staff only via the SDSU Tableau Server website. Authorized data users can also access record-level data at the individual (e.g., student demographics), class/instructor (e.g., grade distribution) or unit level (e.g., unit budget) via the mySDSU Query Viewer. These data venues provide a wide range of data, including admission, enrollment, student performance, retention and graduation, degree completion, and demographic distributions of students, faculty and staff.

For data that are NOT available via the aforementioned channels, a data request must be completed.

1. **Request institutional data**: The Data User should complete the Data Request Form (in development). The request will be routed to the requestor's supervisor for approval and the request will be evaluated against the requestor's existing role-based security. Completion of FERPA training will be required for all requestors. If their current role-based security allows for access to the requested data, then the request will be assigned to the appropriate Data Steward and the User will receive an acknowledgement (and additional justifications and/or clarifications as needed). If those data requested are outside of approved role-based

security, the request will be reviewed by Data Trustees. Upon Data Trustee approval, the request will be routed to the appropriate Data Steward for processing. If needed, Data Trustees and DGTC will be consulted to determine the appropriateness of a data request. Large-scale, complicated, sensitive and/or unprecedented data requested will require the approval of the DGTC.

2. **Access to user-specific dashboards:** Some dashboards – located either in the Tableau Server or mySDSU – are accessible to only certain individuals. To access these dashboards, the Data User should complete the Tableau Access Request Form. The form will be reviewed by ASIR within 1-2 business days, and routed to the appropriate Data Stewards for approval. The Data User will receive an acknowledgement once the request is processed, and additional justifications and/or clarifications may be requested.

3. **Access to campus data warehouse:** Proposed future project, Data Infrastructure & Insights Initiative (DI3)

VII. Data Sharing and Storage[2]

Data sharing allows for collaboration that is critical to many campus units' operations. The University has a wide variety of institutional data that fall into different security levels, and follows the SDSU IT Security Office link.

Data are shared via a range of tools for collaboration, sharing, and storage on campus. General guidelines for using the appropriate tools should be followed to ensure the broader best practices of data privacy and security are followed. ITSO provides guidance for Sensitive Data Storage Best Practices including Level 1 -3 data as referenced below:

- **Cloud Storage:** Level 2 and 3 data should be stored in Cloud Storage.
- **Secure Internal File Share:** Level 1, 2, and 3 data should be shared and stored for internal use via secure platforms. SDSU IT Security Office provides guidelines on the available options, e.g., google drive and settings for internal sharing.
- **Secure File Transfer:** Level 1 and 2 data should be transferred to SDSU and CSU users using a secure file transfer solution. Currently, **MoveIT** is implemented at the CO to transfer files securely. SDSU's tool for sharing externally will be specified once identified.
- **File Encryption:** Sensitive data shared with non-CSU colleagues should be encrypted. Currently, **7-zip** is supported by SDSU to encrypt files.

VIII. Data Retention and Disposition

All Level 1 and Level 2 information must be securely removed from all software and/or computer files as well as storage media devices in accordance with CSU Executive Order 1031. Data users are responsible for managing the retention and disposition of data. Random audits of data storage and destruction will be conducted to ensure adherence.

IX. Metadata - Data Definitions

SDSU will establish an online data catalog as a reference tool for the campus community. The data catalog will support consistent and responsible data use by defining data elements, identifying source systems and use restrictions, linking to published reports and mapping relationships to external accountability frameworks. The catalog will expand on the Data Glossary currently maintained by Analytic Studies and Institutional Research (ASIR). ASIR will continue to oversee the data catalog. Data Experts will contribute to the catalog, creating and maintaining content in their area of expertise.

SDSU may explore options for automated metadata generation, as part of the future data warehouse project.

[2] Reference websites: https://security.berkeley.edu/data-classification-standard; https://services.dartmouth.edu/TDClient/1806/Portal/KB/ArticleDet?ID=64874