CSUF Data Governance Guidelines[1]

I. Background

Institutional data are the foundation for sound decision making for student success and university operations. Data are critical strategic assets of the university, and thus require appropriate governance structure for the collection, management and use of data. As 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.

This guideline exists alongside Federal, State, CSU system, and other campus policies or laws that govern the use of personally identifiable information.

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 best practices for data management and security.
3. Establish a mechanism for documenting a data trail for data access and usage requests.
4. Empower the Institutional Data Governance 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.

The document applies to all institutional data collected or used in the operations of the university and all of its business units. 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. Data collected by campus stakeholders in the course of research and creative activities are not included under the guidelines, with the exception that data collection coordination involving the use of surveys should reference the guidelines available from the university survey website (www.survey.fullerton.edu).

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

IV. Principles

A set of principles guide the CSUF Data Governance Guidelines:

1. **Alignment with university mission:** Institutional data supports the mission of the university, facilitates evidence-based decision-making, and aims at continuous improvement; Personal use of institutional data is prohibited; Use of data that deviates from the university's policies, including diversity, equity and inclusion, is also prohibited.
2. **Transparent guidelines:** Policies and procedures regarding institutional data should be clear, transparent, consistently applied, and implementable.
3. **Sound practices:** Sound record management practices (e.g. records retention, destruction) should be applied to both institutional data and unofficial university records; The systems for institutional data should be well-defined and kept current; Unnecessary duplication of institutional data should be discouraged; Outdated or data no longer in need should be securely destructed; All data-related practices should be documented in an auditable and traceable manner.
4. **Legitimate purposes:** Data should be accessed and shared appropriately only when there is a legitimate business purpose.
5. **Data security:** 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.). Data should be stored in a secure manner appropriate for the corresponding data formats, and accessible only by authorized users.
6. **Data privacy:** Data containing information about individuals should be treated with respect, and follow appropriate data privacy and security protocols.
7. **Data validation:** Data used or shared inside or outside the university should be validated at multiple levels (e.g. by the Data Stewards, Data Custodians) to ensure the quality, integrity and security of data are not compromised.
8. **User training:** Any individuals involved in the handling of institutional data must be properly trained in the relevant regulations and practices.

V. Roles and Responsibilities

Institutional data are owned by the university. They 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 outline below will govern institutional data management, access, accountability, and security.

1. Institutional Data Governance Committee (IDGC)

The Institutional Data Governance Committee is responsible for the oversight of appropriate data processes in support of data-driven decision-making at CSUF. IDGC is charged with developing and updating the campus guidelines regarding data use. In the absence of federal, state, and CSU policy, IDGC is the governing body to make decisions about university data policies. Specifically, IDGC:

- 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 (though not limited to) access to and use of data.
- reviews and approves complex or controversial data access requests.

IDGC is comprised of representatives from university divisions and units who have knowledge of institutional data and best practices in the use of such data. The membership of the IDGC is appointed by the President, and is reviewed and renewed annually:

- The Vice President of Information Technology/Chief Information Officer (Chair)
- The Associate Vice President for Institutional Effectiveness (Co-Chair)
- College representatives (Two Associate Deans)
- Faculty representatives (Two faculty members, preferably from Senate IT committee and/or Assessment and Educational Effectiveness Committee)
- Staff representatives (Two Data Analysts, preferably from Admissions, Assessment and Institutional Effectiveness, and/or Records)
- Student representative (One student recommended by ASI)
- General Counsel
- Information Security Officer
- Director of Risk Management
- Five divisional representatives (One from each of the following divisions: Administration and Finance, Human Resources, Diversity, and Inclusion, Information Technology, Student Affairs, University Advancement)

IDGC is charged by and reports to the President, and its recommendations are forwarded to the President for final decisions. The IDGC should meet once a semester, with the possibility of more frequent meetings as needed.

2. Data Trustees

Data Trustees are members of the senior administration with planning and decision-making authorities for CSUF's institutional data, who typically oversee the collection, generation, management, and dissemination of institutional data. Specifically, they include:

- Campus data infrastructure: Vice President for Information Technology
- Student records: Provost and Vice President for Academic Affairs; Vice President of Student Affairs; College Deans
- Faculty academic records: Provost and Vice President for Academic Affairs; College Deans
- Employee information: Vice President for Human Resources, Diversity, and Inclusion; College Deans
- Development and alumni information: Vice President for University Advancement; College Deans

- Budget and financial data: Vice President for Administration & Finance; College Deans

3. Data Stewards

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 the data governance guidelines within their units. Specifically, the Data Stewards manage access to data for employees within their units. They are responsible for authorizing the request of data access based on the employees' roles, ensuring the employees receive proper training, and monitoring whether the employees successfully and appropriately execute their data access and roles. Specifically, they include:

- Student records: Registrar; Associate Director(s) from the Office of Assessment and Institutional Effectiveness; Assistant Vice President for Enterprise Applications; Assistant Director of Assessment and Student Development
- Student success data: Assistant Vice President of Student Success; Associate Deans of all colleges
- Financial information: Director of Financial Aid; Director of Student Financial Services; Director of Student Business Services
- Admission information: Director of Admissions; Assistant Vice President for Graduate Studies
- Alumni information: Chief of Operations, University Advancement
- Scheduling and workload information: Scheduling Lead
- Faculty academic records: Director of Faculty Affairs and Records
- Employee information: Chief of Operations, HRDI
- Space/Facility information: Associate Vice President of Administration and Finance/Capital Programs for Facilities Management
- Budget operations: Assistant Vice President for Resource Planning and Budget
- Public record request: Public Records Request Coordinator

4. Data Custodians

Data Custodians are individuals within units designated by Data Trustee to have direct physical control over physical or electronic information systems that house institutional data. Data Custodians have operational responsibilities in assisting Data Stewards with day-to-day data related activities, including (though not limited to) collecting, generating, managing, maintaining, distributing and securing institutional data. Data Custodians 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 Custodians 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, and maintaining procedures for the secure disposal of university data.

5. 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, and safeguard the access to identifiable data to authorized individuals.

VI. Data Access

CSUF regularly provides aggregated data about our students, faculty, and staff. Multiple public dashboards are available via the Office of Assessment and Institutional Effectiveness website. CSUF-only dashboards, which provide additional and more disaggregated data, are available to CSUF faculty and staff only via the university 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 university portal. These data venues provide a wide range of data on admission, enrollment, student performance, retention and graduation, degree completion, demographic profiles of student, faculty and staff, and much more.

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

1. **Request institutional data**: The Data User should complete the Data Request Form (http://www.fullerton.edu/data/request/). The form will be reviewed by co-chairs of the IDGC (or their designees) within 1-2 business days, and routed to the appropriate Data Stewards/Custodians for processing. The Data User will receive an acknowledgement once the request is assigned, and additional justifications and/or clarifications may be requested. If needed, Data Trustees and IDGC will be consulted to determine the appropriateness of a data request. Large-scale, complicated, sensitive or unprecedented data requested will require the approval of the IDGC.

2. **Access to user-specific dashboards:** Some dashboards – located either in the Tableau Server or the university portal – are accessible to only certain individuals. To access these dashboards, the Data User should complete the Data Request Form. The form will be reviewed by the Office of Assessment and Institutional Effectiveness 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:** The campus data warehouse hosts a wide variety of institutional data, and reports and data extracts can be created from the data warehouse using query tools. Access to campus data warehouse should be submitted via the IT Data Warehouse website.

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 CSU and CSUF Data Classification standards.

Data are shared via a range of tools for collaboration, file sharing and storage on campus. General guidelines for using the appropriate tools should be followed to ensure best practices of data privacy and security are followed.

- **Cloud Storage:** Level 2 and 3 data should be stored in Cloud Storage. Currently, **Dropbox** is approved for storing Level 2 and 3 data, but Level 2 data should not be stored in a file that is shared with non-CSUF users.
- **Secure Internal File Share:** Level 1, 2, and 3 data should be shared and stored for internal use via secure platforms. **FileCloud** is currently being implemented to provide a secure platform.
- **Secure File Transfer:** Level 1 and 2 data should be transferred to CSUF and CSU users using a secure file transfer solution. Currently, **MoveIT** is implemented to transfer files securely.
- **File Encryption:** Sensitive data shared with non-CSU colleagues should be encrypted. Currently, **7-zip** is implemented to encrypt files.

For more information on data sharing and storage, please see the CSUF ISO guidelines on Securely Transferring Data.

VIII. Data Retention and Disposition

All Level 1 and Level 2 information must be securely removed from all software and/or computer files, and storage media devices in accordance with CSU Executive Order 1031. It is the responsibility of the data user to manage the retention and disposition of data.

The CSUF Information security officer randomly audits the data request, storage and destruction process on campus.

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