CHAPTER ONE

UNIVERSITY ORGANIZATION AND CAMPUSWIDE POLICIES

# DATA MANAGEMENT

## Overview

Data are valuable Cal Poly assets. Data have essential value when applied to make decisions or support university operations. Data also have calculable monetary value. Like any asset, data must be maintained, governed, and managed to provide and retain its value.

Data assets must be shared to maximize their value to the Cal Poly community. As a state university, Cal Poly is governed by privacy and security laws and regulations that require policies, procedures, and other controls be established to protect data from unauthorized use or dissemination.

The Cal Poly data environment is best described as a data republic. In the data republic, data needs and requirements are submitted by users to the centralized Office of Data Management (ODM). The mission of the ODM includes:

1. Improve data management by clearly defining roles, policies, and procedures.
2. Maximize data availability across campus through a managed data environment.
3. Create and nurture a culture of collective data ownership and stewardship that adheres to the university policies and procedures.

## Cal Poly Data

Cal Poly Data is all data created, collected, purchased, stored, processed, and used by Cal Poly officials and employees for Cal Poly business.

Responsibility for Data acquisition, storage, use, and protection is extended to University employees, and in certain cases, students to support and accomplish the mission of Cal Poly.

Every data user is a steward of that data, responsible and accountable for appropriate use and protection of the data they create, use, and/or process.

Data ownership is defined as having legal rights and control over a set of data. No one person or unit at Cal Poly owns Cal Poly Data. Any monetary or other value inherent to Cal Poly Data belongs to the State of California. Ownership may be shared in the case of Intellectual Property (IP).

The President of Cal Poly is the senior executive accountable for the creation, acquisition, control, and use of Cal Poly data. The President is granted access to all Cal Poly Data unless that access is explicitly prohibited by law, regulation, or policy. The President is also responsible for ensuring Cal Poly Data is governed, managed, and protected on behalf of the citizens of California, university employees, students and the individuals whose personal information is contained within the University data.

### Data Management Governance Organization

#### Office of Data Management

The Office of Data Management (ODM) is the central office responsible for data use, management and oversight. The ODM is an equal advocate for all Cal Poly Data users in all data matters.

The ODM is responsible for:

1. Drafting and implementing the organization, policies and procedures for data management and data governance.
2. Enabling and supporting a culture of data sharing, where appropriate.
3. Designing, implementing, and maintaining the university data architecture.
4. Working with Information Technology Services (ITS) and data users to identify, implement, and maintain data analytic and business intelligence tools and techniques.
5. Improving data and system efficiencies by identifying duplicative data sources, tools and projects; consolidating, eliminating, and terminating as appropriate.
6. Working to decrease cost of collecting, managing, and sharing data while increasing the value of Cal Poly Data
7. Providing expertise and consultation on all new major data-related or data-intensive initiatives

#### Executive Data Steering Group

The Executive Data Steering Group (EDSG) provides overall University strategy for the collection, consumption, storage, and business use of Cal Poly Data. The EDSG is made up of Cal Poly Executives and is chaired by the CDO.

152.2.1.3 Data Management Council

The primary function of the Data Management Council (DMC) is to operationalize the campus data strategy, and apply it to daily business practices. The DMC recommends policy actions, and coordinates changes to the data architecture.

The DMC is made up of Data Authorities from Academic Affairs (AA), Student Affairs (SA), Administration and Finance (A&F), University Development (UD), Information Technology Services (ITS), Office of University Diversity and Inclusion (OUDI), and the Office of the President.

#### Data Management Working Group

The Data Management Working Group (DMWG) identifies, collaborates, coordinates, and makes recommendations to resolve data management issues.

The DMWG is comprised of campus Data Experts and Data Managers.

## Data Management Roles

### Chief Data Officer

The Chief Data Officer (CDO) is a senior member of the University Staff, accountable for all campus data management activities.

The CDO manages the ODM.

### Organizational Data Roles

Each campus division will assign resources to staff the organizational data management roles. These roles may be filled by a single person, or multiple people.

152.3.2.1 Data Authority

The Data Authority is empowered to make data decisions for their organization. These decisions include definitions, formats, and business use rules. Their authority is formally delegated by the campus executive for whom they represent. The Data Authority may further delegate this authority within their organization, as appropriate.

152.3.2.2 Data Manager

The Data Manager in responsible for implementing University data management policies and procedures within their organization. A current list of Data Managers is held and maintained by ODM.

Data Managers implement and ensure compliance with data access security standards through staff training. They also assist in data interpretation training and are responsible for annually reviewing the approved data security for individuals in their respective organizations.

152.3.2.3 Data Expert

Each division will appoint one or more Data Experts. Data Experts are knowledgeable about all aspects of their organization’s data. They are typically functionally aligned, and have expertise in the laws, regulations, policies, and security practices that govern the data for which they are responsible. They are aware of each system that processes the data, the purpose of those systems, and how the system uses the data. Data Experts review access requests, and make approval recommendations. A list of current Data Experts is maintained by the ODM.

Data Experts have specific responsibility to:

1. Understand and apply appropriate laws, regulations, policies and guidelines of the United States, the State of California, the California State University system, and the University.

2. Adhere to data standards developed by Information Technology Services (ITS) on such matters as data element naming conventions and standard abbreviations, and take steps to assure the integrity, accuracy and completeness of data.

3. Recommend policies and establish procedures and guidelines to protect and maintain the accuracy and integrity of data subsets.

4. Implement and maintain appropriate security over data.

5. Actively participate to resolve issues that emerge when more than one Data Expert claims responsibility for the same data elements. Disputes will be resolved by the DMWG.

152.3.2.4 Data User

A Data User is any current Cal Poly employee or student who has lawful and appropriate access to Cal Poly Data. All users must adhere to Federal, California, California State University system, and Cal Poly laws, regulations and policies regarding access, and must maintain the privacy and security of data.

152.4 Data Access

Access to Cal Poly Data must be as open as possible to make the data most useful. Data sharing for internal use is encouraged among authorized users. Data Access, however, must be controlled to help ensure security and compliance.

Data Access refers to incidental, frequent, or permanent disclosure or provision of data to a person or system. Data Access is typically provided by a report, dashboard, or open access of approved data sets to users or systems.

152.4.1 Data Access Requirements

Data Users must have the Right and Need to know the data, and be properly trained, before data access may be granted.

152.4.1.1 Right-to-Know and Need-to-Know

Access to data will only be given to those that have both a Right-to-Know, and a Need-to-Know.

Right-to-Know is determined by the role the person being given data access has at Cal Poly. Cal Poly employees are considered California officials, and generally have the Right-to-Know. Consultants, vendors, and other third party organizations may have the Right-to-Know if they are engaged in contracted activities in support of Cal Poly.

Need-to-Know refers to whether there is an approved business need for access to specific data. Need-to-Know is certified by the management chain of the person to which data access is being considered. Need-to-Know for Level III data may be certified at the supervisor level, or above; Level II data at the Director level; and Level I data at the Assistant or Associate Vice President/Provost (AVP) level, depending on the organization.

Explanation of data security levels is found in the Cal Poly Information Security and Responsible Use Policy

Students may occasionally have an academic need to access Cal Poly Data. Students acting on behalf of themselves are not California officials and therefore do not have the Right-to-Know for Level I and Level II data. Student employees may have a Right-to-Know if data access is required as a part of their employment. The ODM will review all Student data access requests and determine whether Right-to-Know and Need-to-Know exists.

Data Managers will conduct an Annual Access Review for all data users within their organization to ensure those users have a continued Need-to-Know.

152.4.1.2 Training

Access to student-related data will only be granted to people who have first completed Family Educational Rights and Privacy Act (FERPA) training and Security Training. FERPA and Security trainings are available online through the Learning Hub.

Additional training, specific to the data requested, may be required. Training requirements are determined by those Data Expert(s). The same Data Expert(s) are responsible for ensuring the training is successfully completed.

152.4.2 Data Access Requests

The ODM has oversight and management responsibility for the Cal Poly data access approval or denial process.

ODM will establish and maintain a central, automated Data Access process for all data access requests.

Data Access Requests will normally be processed and completed within five business days of submission. Completion includes: submission of request; review by relevant Data Experts; completion of any additional training required; recommendation for approval or denial of access; and data access given. It is understood that on occasion this timeline may not be possible because of work conflicts, vacations, or illness. In those cases, every effort will be made to complete the request in 10 business days. Requests not complete in eleven business days will be escalated to the CDO for resolution.

152.4.2.1 Request Submission

Data Access requests will be submitted by the appropriate manager, based on the classification of the data. Submission by the manager certifies the Right-to-Know and the Need-to-Know of the person begin granted access. Submission also certifies that the person has received FERPA and Security training.

152.4.2.2 Request Review

Data Access requests will be routed to the Data Expert cognizant for the data requested. The Data Expert will review the request to:

1. Ensure use of the data for the purpose described in the request will not violate any laws, regulation, or policies.
2. Ensure the person being given access has received any required training beyond FERPA.
3. Mitigate, as much as possible, conditions that would otherwise result in denial of the request.

The Data Expert will forward the request to ODM with a recommendation for approval, or denial, of access.

152.4.2.3 Request Approval/Denial

Data Access requests recommended for approval by the Data Experts will be forwarded to ITS or the appropriate office for fulfillment.

Data Access requests recommended for denial by at least one Data Expert will be forwarded to the ODM for final determination.

Only the ODM can deny a data access request.

152.4.3 Data Profiles

Cal Poly employees require routine access to Cal Poly Data based on the position they fill and their role in the University. Access requirements may change as an employee changes position.

Data Profiles will be established and maintained for each Cal Poly employee position. The profiles will establish minimum data access requirements for the employees filling those positions. As an employee transfers from one position to another, the Data Profile will be used to grant or revoke access as documented in the Profile.

The profile will include names of those data systems and data sets required by the position. The will also include incumbent employee identification information as well as FERPA and Security training completion dates. Access will not be given until FERPA and Security trainings are complete.

152.5 Data Distribution

Data Experts will review all data intended for distribution or publication outside of Cal Poly channels to ensure compliance with security, legal, and regulatory requirements. This includes documents, data files, reports, presentations, and public postings (including web sites, social media, etc.) released to third parties, vendors, other CSU campuses, and the public.

Institutional Research (IR) will also review those documents to ensure they do not conflict with other University reporting.

Collaboration with Data Experts and IR during document preparation is encouraged.

152.6 Data Standards and Conventions

Data must adhere to technical and operational Standards and Conventions to be accurately processed by information systems.

152.6.1 Data Definitions, Standards and Conventions Responsibilities

ITS is responsible for defining technical data definitions, standards and conventions for all campus systems.

ODM is responsible for defining operational data definitions, standards and conventions for all campus systems.

ODM will publish and maintain a data catalog containing technical and operational definitions, standards and conventions. The data catalog will be the single source for these definitions.

152.6.2 Personal Names and Pronouns

A person’s name is a basic, important part of their identity. Many people embrace their legal, given name as their identity. Others prefer to be known by something other than their legal name because it best reflects their personal identity. Where possible, Cal Poly Students, Faculty, and Staff may choose to use a preferred first, middle, and last name in directories, lists, and other documents and databases. This is not an option for those directories, lists, databases, and documents that require legal names (i.e., payroll, etc.).

Cal Poly Students, Faculty, and Staff may use personal pronouns of their choice.

References for CAP 152:

1. Date approved by the President: TBD
2. Effective Date: TBD
3. Responsible Department/Office: Office of Data Management
4. Revision History: Not applicable/New
5. Related University Policies, Procedures, Manuals and/or Documents:
6. Cal Poly Information Security and Responsible Use Policy
7. Laws, Regulations and/or Codes of practice referred to herein or related to this policy:
   1. Higher Education Act of 1965, Amended
   2. Family Educational Rights and Privacy Act of 1974 (FERPA), Amended
   3. Title IX of the Educational Amendments Act of 1972 (Title IX), Amended
   4. California State University Information Security Policy 8000