



COLLEGE of CENTRAL FLORIDA
ADMINISTRATIVE PROCEDURE

Title: Data Governance	
Page 1 of 4	Implementing Procedure For Policies #3.21, #3.24, #3.25
Date Approved: 5/29/14 Date Revised: 9/24/18	Division: Institutional Research and Effectiveness

PURPOSE

Integrity of data is a shared responsibility. This document establishes data governance standards and identifies roles and responsibilities of personnel charged with ensuring appropriate use and accuracy of data to support institutional priorities.

This data governance procedure applies to all college employees and users of college data. Individuals working for institutions affiliated with the college are subject to the same rules when they are using the college data or have any means of access to college data that has been classified as confidential or private.

DEFINITIONS

Data Governance is defined as the overall management of the availability, usability, integrity, and security of the data employed in an enterprise.

Data is information concerning all aspects of college operations that is gathered, produced, stored, and/or disseminated. It includes, but is not limited to, financial data, personnel data, student data, and facility data.

STRUCTURE/ ROLES AND RESPONSIBILITIES

The Data Governance structure at the College of Central Florida is made up of:

- Data Governance Committee
- Data Trustees
- Data Stewards
- Data Managers
- Data Users
- Data Custodians – Information Technology
- Director of Institutional Research and Effectiveness (*Chief Data Officer*)

Data Governance Committee

Cross-functional committee responsible for implementing the procedures related to the Data Governance policy. Reviews operational effectiveness of Data Management policies and

procedures and makes recommendations to the Data Trustees for improvements or changes. The committee is comprised of Data Stewards and designated Data Users or Data Managers. Members share best practices, address cross-functional concerns and ensure communication of operational changes to all stakeholders as appropriate. The committee works to support a college wide, data-informed culture that promotes student learning and success.

Data Trustees

Executive staff with decision-making authority for all institutional data and responsibility for overseeing the continuous improvement of Data Governance and management.

Data Stewards

Management Team level staff with responsibility for individual departments where data is collected, maintained and/or shared for purposes of day-to-day operational decision making. Data Stewards ensure Data Governance policies and procedures are followed within their departments. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access.

Data Managers

Have operational responsibilities in assisting Data Stewards with day-to-day data administration activities, including, but not limited to, developing, maintaining, distributing and securing institutional data. Data Managers are expected to have high-level knowledge and expertise in the content of data within their area of responsibility.

Data Users

Any staff who have read/write access to any institutional data for the purpose of inputting, editing, deleting and analyzing in support of their job functions. Data Users are primarily responsible for data accuracy and integrity.

Data Custodians – Information Technology

Information technology experts assigned to manage and program the systems which maintain institutional data. Data Custodians establish, maintain and oversee the technological infrastructure, movement, storage and security of data to ensure that data is made available to users. Data Custodians work with the Director of Institutional Research and Effectiveness and Data Stewards to develop automated processes which identify erroneous, inconsistent, or missing data and to resolve data issues.

The Director of Institutional Research and Effectiveness has responsibility for guiding effective Data Governance practices with a focus on data quality. The director chairs the Data Management Committee and serves as liaison to Data Stewards. The director works with the Data Stewards to develop data definitions, define how metrics are calculated, and report data discrepancies and inconsistencies for resolution.

OWNERSHIP

All administrative data is owned by the college. As such, all members of the college community have the obligation to appropriately use and safeguard the asset, in all formats, at all times and in all locations.

ACCESS, USAGE AND SECURITY

Data Governance falls within the guidelines of the college's information security procedures which provide details about standards for the protection and use of information and technology resources. Data Governance is even more specialized, referring to specific data sets aligned with functional areas.

- Employees shall have access to the institutional data needed to perform their responsibilities. Institutional data must only be accessed and used by authorized staff in accordance with Information Security Policy 3.24.
- Individually identifiable data shall be available to the extent necessary to perform duties.
- Institutional data must only be used for the purpose for which its use has been authorized.
- Authorization of access to data is not transferable.
- It is the responsibility of the user to understand the data they use, and to take necessary steps to prevent misrepresentation or inaccurate interpretations of data.
- The Director of Institutional Research and Effectiveness and Data Stewards work together to ensure that departmental procedures address specific access permissions and use of data in respective areas. Data Trustees review and approve procedures as needed.
- Extraction, manipulation, and reporting of institutional data must be done only for college business or as approved by Data Trustees.
- Personal use of college data without appropriate permissions in any format is prohibited. For example, the use of data in dissertation research must be approved through the college's Institutional Review Board process.
- All data users are expected to be familiar with and conform to the following related college policies and their accompanying procedures:
 - Policy # 3.21 – Technology Use
 - Policy # 3.24 – Information Security
 - Policy # 3.25 – Appropriate Use Policy/Information Technology Resources
 - Data Loss Prevention Procedure
 - Information Security Procedure
 - Appropriate Use Procedure

INTEGRITY AND INTEGRATION

Recognize that data is only as good as its accuracy and use in decision making.

Data Stewards and Data Managers are responsible for developing a plan for their departments to assess the risk of erroneous or inconsistent data and develop a plan to correct inaccuracies.

Data processes used to develop institutional reports must adhere to data validation rules that ensure the highest levels of data integrity are achieved. The Data Governance Committee will ensure compliance with validation rules. These include checks and balances such as manual staff review and programming to meet expected outcomes, data verification for consistency, reasonableness and accuracy.

Vice President, Institutional Effectiveness
and College Relations

Date

Approved by President

Date