



## **AP-3240 Data Governance**

**References: BP-3240 Data Governance**

### **Purpose and Scope**

Institutional data is a valuable asset to all stakeholders of Rogue Community College (RCC) and enables it to assess the needs of the college community, make decisions to maximize the impact of its services to learners, and provide the best value to taxpayers. It is vital not only in the day-to-day operations of the College but to short-term and long-term planning, and it serves as the basis for internal and external reports.

These procedures and guidelines apply to all RCC students, faculty, staff, administrators, consultants, vendors, authorized guests and to any other persons granted use of the College's data assets.

### **Data Integrity and Consistency**

Data collected and maintained by the college in all modalities shall be consistent with the practices, recommendations, and guidelines of the appropriate regulatory authorities including, but not limited to, the Northwest Commission on Colleges and Universities, the Oregon Higher Education Coordinating Commission, and the United States Department of Education/National Center for Education Statistics. Data elements related to current and former students shall be stored in formats that are substantively in compliance with the college's mandatory reporting requirements to accreditors and state and federal regulators.

### **Single Source/Version of Truth**

To ensure data accuracy and consistency across the institution, RCC designates its Enterprise Resource Portal (ERP) and any designated auxiliary systems collectively as the "single source/version of truth" for all core operational data, including but not limited to data related to students, employees, vendors, finances, and physical and digital assets.

### **Data Roles**

Appropriate stewardship and safety of institutional data is ensured by assigning different levels of role-based access determined by job function. New employees and authorized contractual personnel are provided access consistent with their roles during the onboarding process; existing employees are provided access consistent with their current responsibilities; the level of access maybe modified as the responsibilities of the employee change. Access control to the different roles is maintained by the Chief



Information Officer or designee via a ticketing system. It is possible that the same individual may have more than one of the following data roles depending on that individual's job functions:

*Data Owner* (President, Vice Presidents, Deans, Directors): Data Owners have ultimate authority and decision-making responsibility over a particular collection of college data. Responsible for changing and/or delegating correction of data errors, adhering to college data quality policies and standards, determining data metrics, and assigning resources for data management activities. The data owner has a sound business understanding, an in-depth knowledge and awareness of the regulations, policies, laws governing data privacy of the data they own.

*Data Steward* (Institutional Research Analysts, Functional Analysts, Department Technology Specialists): Data Stewards act under the authority of Data Owners and understand the business needs and rules of the data for their respective areas and understand how it is used on a day-to-day basis. They are often responsible for transmitting compliance-related data to outside regulators and recommend to Data Custodians steps for ensuring the accuracy of information and correction of data errors, creating and maintaining documentation and ensuring data standards are maintained.

*Data Custodian* (Information Technology and Institutional Research Analysts): Data Custodians directly access and manage the database(s) and data management systems and resources of the college in support of college operations. They are responsible for maintaining and protecting data integrity and unauthorized access, maintenance and updating of relevant documentation, making data available for others to use, participating in preparation and testing of database upgrades in assigned areas, and partnering with data owners and data stewards to enhance data quality and access.

*Data Analyst* (Support Personnel, Administrative Specialists, Audit Personnel): Data Analysts are responsible for using accessible data to execute their various day to day job functions including, but not limited to, analysis, projection, presentation, and budgeting.

*Data User* (All other authorized individuals): Data Users are personnel whose routine job duties require the use of data points available in the various data repositories and data systems of the college.

## **Data Governance Committee**

Under the aegis of the President or her/his designee, the college's Data Governance Committee (DGC) is responsible for the strategic direction of the data governance protocols of the college. The DGC meets regularly on a schedule to review data governance policy and procedures for maintaining standards, currency, regulatory compatibility, integrity, privacy safeguards, and industry best practices related to institutional data. The DGC also serves as the clearinghouse and coordinator for vendor-



generated and/or vendor-recommended updates and patches for the ERP, any ERP-related ancillary or auxiliary information systems, and any other data systems or platforms that may interface with the ERP in the routine operations of the college. The DGC serves as the primary forum for discussion and recommendation on ERP life-cycle stages. As necessary, the DGC recommends to the appropriate college leadership changes to policy, procedures, and practices related to institutional data storage and handling.

**Rescinds Procedure Number: None**

**Approved: December 5, 2023**

**Revised: April 1, 2025**