

DATA GOVERNANCE

I. Policy Section

3.0 College Operations

II. Policy Subsection

3.10 Data Governance

III. Policy Statement

Data governance establishes standards and provides expectations for effective management of institutional data at Grand Rapids Community College (GRCC). Institutional data is used for internal assessment and mandatory reporting as well as the efficient and impactful operation of GRCC.

Institutional data must be secure and available to those who are permitted to use it. GRCC's data governance applies to institutional data upon initial collection and/or creation. All GRCC faculty, staff, students, affiliates, and contractors are responsible for following the expectations of their data governance role when using institutional data.

IV. Reasons for the Policy

Responsible management of institutional data is critical to the work of the institution and required in order to ensure those with official educational or administrative responsibilities are able to access reliable and agreed upon data as well as maintain expected privacy and security.

V. Entities Affected by this Policy

This policy applies to all GRCC faculty, staff, students, affiliates, and contractors.

VI. Who Should Read this Policy

All GRCC Employees
Students
Affiliates
Contractors

VII. Related Documents

3.1 Institutional Review Board
3.6 Records Management
3.7 Contracting Authority
6.18 Acceptable Use of Technology
6.19 Freedom of Information Act (FOIA)
8.6 The Family Educational Rights and Privacy Act (FERPA)

14.3 Complaints Regarding Violations of Privacy and Confidentiality (HIPAA)
Records Retention
15.1 Personally Identifiable Information
Federal Grants Data Governance disclosure
Types of Data Classifications
GRCC Information Security Program

VIII. Contacts

Policy Owner: Director of Institutional Research (IR)
Registrar
Chief Information Security Officer
General Counsel
Director of Grants Development
Controller
Executive Director of Human Resources

IX. Definitions

A. Institutional Data

Information created, collected, stored, maintained, transmitted, enhanced, and/or recorded by GRCC in our campus wide information system and systems using the data for other business functions including, but not limited to, student information, financial information, employee information, and research data.

B. Data Governance Council

Cross-college team comprised of the College Data Officer, Chief Information Security Officer, data officers, data stewards, and data users, responsible for defining, implementing, and managing the data strategy related to institutional data sets.

C. Data Officers

Typically, leaders of departments, these are individuals with direct tactical oversight of and responsibility for specific institutional data sets.

D. Data Stewards

Employees with technical and/or functional knowledge of defined institutional data sets.

E. Data Users

Individuals who are using institutional data sets, primarily for making data-informed decisions.

X. Procedures

All GRCC faculty, staff, students, affiliates, and contractors are considered data users. And they must:

- Immediately communicate any unauthorized access or data misuse to an Information Technology security team member
- Maintain protection of data in accordance with college data security policies.
- Use institutional data appropriate for their role.
- Follow the policies and procedures established to store data under secure conditions in accordance with college data security.
- Comply with federal and state laws and regulations and college policies, procedures, and data privacy standards.
- Report any concerns regarding data quality of institutional data to the Data Governance Council.

XI. Forms

Institutional Research Data and Service Request Form
Contractor Agreement
Data access approval form
FERPA acknowledgment form
FERPA addendum
Data Sharing Agreements

XII. Effective Date

March, 2026

XIII. Policy History

October, 2023 - Policy Implemented
March, 2026 - revised

XIV. New Review/Revision Date

March, 2028