ROLLINS COLLEGE POLICY

Title: Data Governance	Type: Data Governance
No: **DG 1101**	Approval Date: 2-9-2023
Responsible Office: Office of Institutional Analytics	Reviewed By: Data Governance Committee, 9-9-2022; Policy Committee, 12-13-2022; President's Cabinet, 2-9-2023 Approved By: President, 2-9-2023
Next Review: 2026-2027	Revision No:

I. Purpose/Introduction/Rationale

Rollins College recognizes that its data is a strategic asset, and the efficient use of that data is critical to the institution's success. Rollins College also recognizes that consistent, repeatable, and sustainable processes for managing data reduce inefficiencies, promote good stewardship of resources, and reduce risk to the institution. The framework below for data governance has been established to ensure that information is secure, accessible, and reliable.

The data governance framework is intended to achieve the following goals.

- Define the roles, responsibilities, and accountability for all parties involved in collecting, using, and disposing of data critical to Rollins College.
- Develop procedures, standards, and processes for effective governance of data.
- Protect Rollins College data from internal and external threats.
- Ensure that the use of data complies with applicable laws, rules, and regulations.
- Ensure that data architecture is created and maintained in such a way that it is resilient, integrated, and meets the future information needs of Rollins College.
- Ensure processes are in place to create and maintain data quality

The data governance framework applies to all data acquired, disseminated, used, shared, curated, or disposed of by Rollins College. Data governance also applies to all third parties who receive, disseminate, use, share, curate, or dispose of data provided by Rollins College.

II. Definitions

Data Governance. A framework establishing control and accountability over data assets. The framework extends to the acquisition, dissemination, use, sharing, curation, disposition, integrity, and Security of all data. The framework is defined by policies, procedures, standards, and practices and is aligned with the strategic plans of Rollins College. It applies to data falling within ***either*** of the following categories:

1) most critical data to Rollins College and/or
2) data shared by multiple units within Rollins College.

Data Governance Committee (DGC). The DGC is accountable for developing and monitoring data policy and recommends courses of action related to data management to the institution's senior leadership. The DGC is also responsible for supervising the activities of each subcommittee, working groups, stewards, custodians, curators, and users to ensure that information procedures, standards, and practices are followed with the College's Data Governance Framework.

Chief Data Officer (CDO). A member of the leadership team that guides the data governance process. The Chief Data Officer (CDO) is a position within the institution responsible for creating value from institutional information assets.

Data Governance Operation Team. This team is responsible for providing operational support to Data Governance. The team includes the Chief Data Officer, Chief Information Officer, Sr. Director of Institutional Analytics, Director of Enterprise Data, IT Data Analyst, Director of Enterprise Applications, Institutional Research Specialist, Director of Business Process Improvement, and the Data Coordinator. Except for the Chief Data Officer and the institutional Research Specialist on the Data Governance Operation Team, everyone else on this team are attributed as "ex-officio" members of the Data Governance Committee and has no voting privileges.

Domain Trustee. Domain Trustees are high-level academic or business members who are part of the President's Cabinet that has authority over policies, procedures, standards, and practices regarding data curation, use, and access.

Data Governance Committee (DGC) Meeting Facilitator. A Meeting Facilitator is an ex-officio member who plans, organizes, and runs the data governance committee meetings in collaboration with the Data Governance Operation Team and other guest members of the Rollins community involved in specific business cases.

Data Steward. Data Stewards are academic or business members of the institution appointed by a Domain Trustee. For data governance purposes, Data Stewards report to the Data Governance Committee. Data Stewards are academic or business members of the institution appointed by a Data Trustee. For data governance purposes, Data Stewards report to the Data Governance Committee.

Data Curator. Data Curators are members of the subject area and business domains responsible for data quality in systems of record. Data Stewards appoint Data Curators.

Data Custodian. Data Custodians are members of the Information Technology team who operate and administer the College's information systems, including systems of record and information repositories.

Data Consumer. Data Consumers include anyone who uses institutional data. Data Consumers are to use data per data governance policies, procedures, standards, and practices and should treat all data as an asset of the College.

Information Security Liaison. Information Security Liaisons (ISL) are the primary point of contact for units concerning data security. The ISL is appointed by the dean, director, or department head. The ISL coordinates with the Information Security Officer or equivalent to implement the institution's data security and data governance policies, procedures, standards, and practices within the unit.

Information Security Officer (ISO). The Information Security Officer (ISO) protects data assets across the institution. The ISO is an advisory member of the Data Governance Committee.

III. Procedure or Application

A. Values

Rollins College uses the following values to guide information governance.

1. Rollins College has a shared vision for data that is aligned with institutional strategy
2. Data should be of sufficient quality to instill trust among data users
3. The Rollins College community is encouraged to use institutional data to improve student success and operational efficiency
4. Security and privacy of data should be maintained and enforced by all data users
5. Data quality issues are resolved in a consistent and strategic manner
6. Transparency and understanding of data assets and processes are critical to successful data governance
7. Data used across units is shared rather than creating duplicate and/or competing data

B. Principles

Rollins College has adopted the following general principles to guide the governance structure.

1. Data Ownership. By default, data assets belong to Rollins College, not any application, department, or individual.
    - The practice of internal data "ownership" or restricting the business use of data due to perceived regulatory limitations constrains its value to the organization and, therefore, the organization's performance. Rollins College strives to make data available to optimize operations in support of the College's mission.
    - Rather than data ownership, individuals performing data governance roles should focus on the responsible use of data and the reduction of data "silos."
2. Data is an asset.
    - Rollins College recognizes that data is used to optimize resources, increase efficiency, and generate revenue. College leaders should use data assets like other institutional assets that hold monetary value. All data users should manage and protect data assets with the same discipline as other college assets.
    - The creation and maintenance of an inventory or registry of all data that is captured, stored, or otherwise available to the organization is of paramount importance in managing data as an asset.
3. Resources.
    - The Data Steward is responsible for ensuring data quality at its source.
    - The Data Steward and Data Curator(s) are responsible for optimizing the usage and understanding of data.
    - The Data Governance Operation Team is responsible for optimizing the availability and utility of data.
    - Information Technology (IT) assists in data governance by enabling enterprise-level data accessibility, availability, and Security based on end-user needs.
4. Data acquisition. An information asset should be acquired or retained only if its actual or planned value exceeds its cumulative cost or as required by laws or other regulations.
    - Data stewards should be deliberate in assessing the value of acquiring a new data asset to ensure that the cost of developing and maintaining the data asset matches its value.

C. Framework

The Data Governance Framework is composed of four key areas.

1. Policies and Standards: establishes the roles and responsibilities of those involved in data management.
2. Compliance and Security: Assess risks to Rollins College data and define the controls necessary to mitigate risk.
3. Data Quality: ensures the stewardship and integrity of the institution's data.
4. Architecture and Integration ensure that data is consistent and defined to allow easy use of the data.

D. Structure

Data governance is overseen by the Data Governance Committee (DGC). The DGC comprises members from the Rollins community who represent the following data domains. *

- **Chief Data Officer (CDO)**
- **Academic Activity Data**
- **Advising Data**
- **Financial Data**
- **Student Accounts Data**
- **Business Processes and Improvement**
- **Library Data**
- **Dean's representative (Faculty data)**
- **Survey Data**
- **HR (Human Resources) and Payroll Data**
- **Admission and Enrollment Management Data**
- **Curriculum, Degrees, and Academic Data (DegreeWorks)**
- **Financial Aid Data**
- **Student Activity and Engagement Data**
- **Institutional Advancement Data**
- **Athletics Data**

See Appendix A for the current list of appointments.

Membership Appointments and Terms. Membership of the DGC will be renewed annually, typically on June 1st of each year, but divisional vice presidents can forward a replacement. In the event of a staffing change, a Domain Trustee can make an off-cycle appointment for a DGC member to fill the vacancy.

The following non-voting members aid the DGC in decision-making. *

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Associate Vice President of IT
- Director, Enterprise Data
- Director, Enterprise Applications
- Senior Director, Institutional Analytics
- Data Analyst, IT
- Data Coordinator, Institutional Analytics

See Appendix A for the current list of appointments.

The DCG will include a Meeting Facilitator from the Ex-officio members who will be responsible for setting and communicating the Committee's agenda and running the meeting.

Meetings and Voting Privileges. The DGC will meet monthly. If an issue arises that requires review before the next meeting, the DGC Meeting Facilitator will schedule a special meeting. The DCG Meeting Facilitator will

designate a person to take minutes at each meeting (currently assigned to the IR Data Coordinator). Minutes from meetings will be distributed on time before the next meeting. Approved minutes will be posted to the DGC website and distributed to key members of the College's leadership.

A quorum for the DGC is at least 50% plus one of the DGC members. The DGC Meeting Facilitator will ensure the list of attendees is robustly maintained.

Each DGC member will do voting. If a member is not available to attend a meeting at which a vote is taken, a designated person may vote in their place. A simple majority must pass an agenda item, and voting results must be included within meeting minutes.

E. Data Governance Roles

The following data governance roles are critical in the success of data governance at Rollins College. Keep in mind that an individual may play more than one role.

1. Data Governance Committee (DGC) Member Responsibilities.
    - Creating and enforcing data policies, procedures, and practices.
    - Endorsing data standards from subcommittees and working groups.
    - Determining what new data will be subject to governance.
    - Overseeing key data activities, such as developing standard reports and dashboards.
    - Ensuring data compliance is maintained throughout the College.
    - Setting goals for the future state of data management capabilities.
    - Advocating for improved data management.
    - Identifying and prioritizing data governance projects.
    - Resolving issues escalated by Data Stewards.
    - Monitoring data quality by reviewing metrics.

2. Chief Data Officer Responsibilities

The Chief Data Officer (CDO) is a position within the institution responsible for creating value from institutional information assets.

- establishing and maintaining an information governance framework
- evangelizing the culture of use of information-informed decision-making
- promoting the use of information as an institutional asset
- mitigating information risk
- aligning an information strategy to the institution's strategic plan
- supervising the enterprise business intelligence function and information and analytics architecture
- aligning information governance with law, rule, and regulation
- creating information literacy programs
- promoting the ethical use of information
- operationalizing information policies, procedures, standards, and practices
- advising the Information Governance Committee on information governance best practices
- setting and enforcing standards for information management technologies and systems, including infrastructure, integrations, information quality, metadata repositories, and access control mechanisms

3. Domain Trustee Responsibilities.
    - Serves as a member of the DGC.
    - Appoints Data Stewards for each subject area domain within the institution.
    - Submits the annual institutional data strategy and progress report.

- Escalates data issues to the institution's senior leadership.
- Recommends and enforces data policies, procedures, standards, and practices.

4. Data Steward Responsibilities.
    - Help to interpret, define, implement, and enforce data management policies, procedures, standards, and practices within their subject area and business domains
    - Identifying systems of record containing institutional data.
    - Categorizing institutional data within systems of record according to data policies, procedures, standards, and practices.
    - Defining data access plans, quality standards, and usage limitations.
    - Reviewing and approving requests for access to data within their subject area and business domain.
    - Documenting and maintaining metadata and assisting Data Curators in evaluating data accuracy and quality.
    - Ensuring data usage complies with laws, rules, regulations, and College policies.
    - Educating the College community on compliance issues and best practices in using the data within their subject area and business domain.
    - Ensuring record retention policies are maintained for data within the subject and/or business practice areas and domains.
    - Enforcing data policies, procedures, standards, and practices within the parameters established by the DGC for the subject and/or business practice areas and domains.
    - Identifying, evaluating, and escalating risks to College data.
5. Data Curator Responsibilities.
    - Ensuring processes for quality data entry within systems of record.
    - Creating/updating metadata definitions and data catalogs as information sources are created/changed.
    - Implementing data access plans, quality standards, and usage limitations.
    - Ensuring data creation and curation comply with law, rule, regulation, and College policies.
    - Following best practices in the curation of data.
    - Participating in working groups created by the DGC.
    - Identifying and evaluating data risks (e.g., data quality, accuracy, and access).
    - Escalating risks to Data Stewards.
    - Providing content expertise for the meaning and usage of data.
6. Data Custodian Responsibilities.
    - Ensuring that transactions in all systems of record are auditable.
    - Providing day-to-day security administration and request fulfillment.
    - Maintaining access records.
    - Communicating appropriate use and consequences of misuse to users who access College systems.
    - Creating, distributing, and following up on security violation reports.
    - Monitoring to ensure the authorized use, Security, and transmission of data.
    - Ensuring designs for new technologies are resilient and aligned with the business needs of the College.
    - In coordination with Data Stewards, implementing and administering controls and procedures to manage application and information security risks.

- Providing access reports to be reviewed and validated by Data Stewards at least once every six months.
- Ensuring that data within systems is protected, and that business continuity plans are in place.

7. Data Consumer Responsibilities.
    - Data Consumers are responsible for the security of the data they consume.
8. Information Security Liaison Responsibilities.
    - Ensuring locally governed data follows policies, procedures, standards, and practices.
    - Promoting security awareness and good security practices.
    - Attending data security awareness and training presentations, seminars, workshops, and events.
    - Disseminating information within the unit to raise awareness about data security issues.
    - Participating in the incident response process (when an incident is within their unit).
    - Creating security risk assessments for locally stored data.
    - Coordinating inventories of sensitive or critical data and information systems.
    - Creating and maintaining business continuity plans for local systems.
    - Assisting in implementing corrective actions resulting from audits or incident reports.
    - Documenting unit security standards and plans.
    - Participating in audits of user security at least annually.
    - Notifying the appropriate Data Steward of changes in personnel or job functions that result in changes to user access.
9. Information Security Officer (CISO) Responsibilities.
    - Staying informed of new laws, rules, and regulations affecting information security and applying those concepts to data governance.
    - Creating, maintaining, and reporting on key performance indicators (KPIs) for information security.
    - Developing and implementing security plans to ensure the protection of enterprise data within source systems and any derivative systems.
    - Implementing security policies and good practices.
    - Establishing a framework for information security.
    - Implementing the data classification scheme as defined by the DGC.
    - Coordinating information security orientation and awareness programs.
    - Managing the Information Security Liaison (ISL) program for information security, including periodic reviews of access.
    - Implementing tools to ensure information security policy and procedures are being applied, and that appropriate audit controls are in place.
    - Auditing information security request fulfillments for accuracy and timeliness.
    - Conducting risk assessments of data and data systems.
    - Acting as a resource for the DGC on information security issues.

F. Documentation

Data governance activities are codified through policies, procedures, standards, and practices.

The DGC recommends ***policies*** to the College's senior leadership to establish critical data governance activities. Policies are created to outline a framework for conducting governance activities.

The DGC, subcommittees, and working groups establish ***procedures*** to formalize how data governance is implemented. While policies outline a framework, procedures define how that framework is implemented to meet governance goals.

The DGC, its subcommittees, and working groups establish and/or endorse standards to instruct Data Stewards and Data Curators on how to care for information appropriately. Standards are designed to describe the actions necessary to achieve a specific goal.

The DGC establishes ***practices*** to ensure the uniform treatment of data. Practices are the decisions made by the DGC on how governance will be applied to specific information within the institution.

IV. Related Policies or Applicable Publications

N/A

V. Effective Date

This policy is effective February 9, 2023, and supersedes all previously issued versions.

VI. Appendices/Supplemental Materials

Appendix A: Data Governance Appointments List

VII. Rationale for Revision

N/A