Data Governance Policy

ROWAN UNIVERSITY POLICY

Title: Data Governance Policy
Subject: Information Resources and Technology
Policy No: IRT:2013:02
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Senior Vice President for Information Resources and Technology and Chief Information Officer
Adopted: 09/01/2013
Last Revision: 08/08/2023
Last Reviewed: 08/08/2023

I. PURPOSE

To set policy for assigning and detailing responsibilities for managing different classifications of university data and to set forth a standard for custodianship of university data. This policy establishes the framework for standards and guidelines to be followed in creation of data storage, destruction, and access mechanisms including data architectures.

II. ACCOUNTABILITY

Under the President, the Vice President for Information Resources and Chief Information Officer (CIO) shall ensure compliance with this policy. The Provost, Executive Vice President for Administration and Strategic Advancement, Vice Presidents, Deans, IR Directors, and individual managers shall implement the policy.

III. APPLICABILITY

1. This policy applies to all individuals accessing University data, including students, faculty, visiting faculty, staff, volunteers, alumni, persons hired or retained to perform University work, external individuals and organizations, and any other person extended access and use privileges by the University under contractual agreements and obligations or otherwise.
2. Data and records stored on University systems are presumed to be the property of Rowan University. Proper stewardship and custodianship of University data will facilitate access to data that supports the work of those with official educational or administrative responsibilities within the institution that is consistent with legal, ethical, competitive, and practical considerations, and will inform users of data of their responsibilities.
3. Nothing in this policy precludes or addresses the release of University Data to external organizations, governmental agencies, or authorized individuals as required by legislation, regulation, or other legal vehicle.

IV. DEFINITIONS

1. *Access* – the right to read, copy, or query data.
2. *Data* – the representation of discrete facts; any information in electronic or audio- visual format, or any hardware or software that enables the storage and use of such information.
3. *Data Administration* – the function of applying formal guidelines and tools to manage the University's data resources

4. *Data Consumers* – employees or agents of the University who access University Data in performance of their assigned duties.
5. *Data Custodians* – University officials and their staff who have operational-level responsibility for data capture, data maintenance, and data dissemination.
6. *Data Dictionary* – a comprehensive repository that defines and categorizes University Data.
7. *Data Stewards* – University officials who have policy-level responsibility for managing a segment of the University's data resource.
8. *Information* – wherever possible, this document refers to data rather than information; Information is defined as a collection of data, ideas, thoughts, or memories.
9. *University Data* – data that is created, acquired or maintained by University employees in performance of official administrative job duties.
10. *University Data Governance Committee (DGC)* – the committee that establishes overall policy and guidelines for the management of and access to the University's University Data in accordance with existing University policies.
11. *University Data Model* – a framework that documents the data entities that comprise the University Database and the relationships among those entities.
12. *Metadata* – data about data that allows for the systematic definition of data and its elements.
13. *Metadata Management* – the process of updating and utilizing the Meta Data to control data related processes and define data in an ever-changing environment.
14. *Record* – data or information in a fixed form that is created or received in the course of individual or University activity and set aside (preserved) as evidence of that activity for future reference
15. *Shared data* – a subset of University Data; data that is maintained by more than one organizational unit.

V. POLICY

1. Regulations, Statuses and Policies
   Responsibility for and access to correspondence and documents created or received by University personnel are governed by the following over-arching policies and legal statutes:

   a. NJ Public Records Law General Statutes
   b. Family Educational Rights and Privacy Act (FERPA)
   c. Health Insurance Portability and Accountability Act (HIPAA) Security Rule
   d. NJ Records Retention Schedule for Four Year College
   e. Americans with Disabilities Act of 1990
   f. The Electronic Communications Privacy Act of 1986 (ECPA)
   g. FTC Red Flags Rules
   h. Gramm Leach Bliley Act (GLBA)
   i. Payment Card Industry (PCI) Data Security Standard
   j. General Data Protection Regulation (EU) 2016/679 (GDPR)
   k. Policy And Procedures On Ethics In Research
   l. Rowan University Information Security Policy and Standards
   m. Rowan University Policy on the Privacy of Electronic Information
2. University Data
   a. University Data is a valuable asset at the Rowan University. It involves all University constituencies (students, faculty, staff, etc.) and resources (funds, space, technology, etc.) that are captured and used in the operations of the University. It serves as the basis for internal and external reports.
   b. University Data enables administrators to assess the needs of the University community and modify services accordingly. It is vital not only in the day-to-day operations of the University but to short-term and long-term planning as well.
   c. Rowan University exercises control over and access to data even when it is technically open under the public records statutes and even though it requires effort and cost to create and maintain access controls. University data is available only on a need-to-know-basis and requires those individuals seeking access to submit a public records request.
   d. To support all aspects of University operations, University data in print and electronic form will be managed as a strategic asset according to “data governance” policies and procedures. University data is a subset of the university's information resources and administrative records, and includes

any information in print, electronic or audio-visual format. This definition includes, but is not limited to, machine-readable data and data in electronic communication systems. It also includes back-up and archived data on all media, and any University data that resides on internal systems or systems hosted outside the control of the University.

e. University data includes data, in any of the forms described above, that is:
    i. Acquired and/or maintained by university employees in performance of official administrative job duties;
    ii. A public record according to the definition included in Federal and State laws;
    iii. Relevant to planning, managing, operating, or auditing a major function at the University;
    iv. Referenced or required for use by more than one organizational unit;
    v. Included in official university administrative reports.?
f. Access to University data needs to be controlled by defining criteria for its governance and creating mechanisms for enforcing policies related to it. Rowan's Data Governance Committee (DGC), chaired by Rowan's Chief Information Officer (CIO), has policy oversight. Distribution of these and related policies, once approved, will be via the Rowan University Policies page on the RU website. ?This policy establishes the framework for standards and guidelines to be followed in creation of data storage, destruction, and access mechanisms including data architectures. ?
g. These data architectures will drive physical implementation of databases and be governed according to the provisions of this document.
h. Data and records stored on University systems may include data from one or more the following areas within Rowan University AND ARE DESCRIBED IN Exhibit 1.

3. Governance Roles
    a. No one person, department, division, school, or group "owns" the data used by the University, even though specific units bear the primary responsibility for some data. The University as an organization owns the data (or in some cases, such as with Social Security numbers, is the custodian of data), but a specific person in the role of the "Data Steward", will be designated with the ultimate responsibility to define how the assigned data is managed within the scope of the legal and regulatory obligations.
    b. The roles and responsibilities assigned to the Data Governance Committee (DGC), Data Stewards, and Data Custodians are included in Exhibits X2, X3, and X4.
4. Responsibilities of Users
    a. Controlling access to University Data is important to protecting the University and its constituency from liability and acts of malice. All public records requests are routed through University Counsel. University employees, faculty, students, and/or agents will be able to access data only after being granted access according to the procedures specified by the Data Steward.
    b. Permission to access University Data will be granted for legitimate University purposes according to the classification of the data being requested and person making the request. Method of delivery, including email and fax, should be carefully considered to ensure data security and compliance. Requests for University Data from an external source or a University employee for non-University purposes will be handled according to the appropriate Federal and New Jersey Public Records Request statues and case law. Users shall respect the confidentiality and privacy of individuals whose records they may access, observe the ethical restrictions that apply to data to which they have access and abide by applicable laws and University policies with respect to access, use, protection, proper disposal, and disclosure of data.
    c. To the extent that the law permits, as determined by the Office of University Counsel, the University reserves the right to deny University Data access to any person or organization that has demonstrated malicious intent or has violated any aspect of the Data Governance Policy.
5. Data Retention and Disposition
    a. Rowan University is a state agency, and its offices and departments are obligated to follow the requirements of the Federal and New Jersey Public Records Law for retention and disposition of records. Rowan will comply with the Gramm Leach Bliley Act, including the data destruction provisions therein, with respect to nonpublic personal information that Rowan obtains in the context of providing a financial service. It should be noted here that University Data might not be destroyed without an approved records retention and disposition schedule that authorizes destruction.
    b. Decisions governing data retention are made based on the content of the data and in conjunction with the department's approved records retention and disposition schedule. Some types of data

may be retained for a long period of time by approved schedules, by policy, or by law. Other types must be purged or destroyed after a certain period of time, again for reasons of preference, policy, or statute. For any circumstance in which data retention is an issue, specific requirements should be clearly documented and should include, at a minimum, the following:

i. The rationale for the retention rule
ii. The timeframe of the retention rule
iii. The method of either saving or disposing of the data according to the retention rule

VI. ATTACHMENTS

1. Attachment 1, Data Classification Matrix
2. Attachment 2, Rowan University Data and Records
3. Attachment 3, Data Governance Committee
4. Attachment 4, Data Stewards
5. Attachment 5, Data Custodians

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer

ATTACHMENT 1

DATA CLASSIFICATION MATRIX

All University Data requires classification with respect to the sensitivity of the data. It is also important to track who is the Steward and the Custodian of the data.

Note that this table is an example and currently defines only a portion of the University Data. A data classification must always take into account the most sensitive data in the collection. Since the data is currently described in such broad groupings, the risk classification is usually the least common denominator of all data elements within a given Area. As the components of each sub area are further detailed, the classification of the data will be adjusted to reflect the appropriate sensitivity of the data subset.

Example Data Classification Matrix			
Area	**Classification**	**Steward**	**Custodian**
Donations	Highly Sensitive	University Foundation	IRT
Clinical	Highly Sensitive	Rowan/SOM	IRT
Student	Sensitive	Registrar	IRT
Employee	Sensitive	HR	IRT
Financial	Sensitive	Finance	IRT
Curriculum	Public	Academic Affairs	IRT

ATTACHMENT 2

ROWAN UNIVERSITY DATA AND RECORDS

Data and records stored on University systems may include data from one or more the following areas within Rowan University:

1. **Alumni Affairs and Development Data**—supports all aspects of alumni and development data. This includes personal data, demographic data, income, and giving data.
2. **Clinical or Medical Data**—supports the management of personal medical information within the University. This data includes patient medical records, benefits, and other related clinical information. Note that HIPAA applies to all personal medical data and patient records of students, faculty, employees, or patients regardless where it is collected or stored. This includes the University's student wellness center(s), health clinics, or related research activities.
3. **Facilities Data**—supports the facilities and services resource of the University including space planning data, construction, maintenance and operational data, reservations, energy consumption data, and physical descriptive data.
4. **Financial Data**—supports the management of fiscal resources of the University and includes accounting, accounts payable, accounts receivable, budgeting, capital assets, investments, inventory, loans, payroll information purchasing, risk management, and treasury.
5. **Human Resources Data**—supports the management of employee resources of the University. This data includes employee demographics, benefits, retirement and EEO data, vitas, employee evaluations, promotion and disciplinary data. Note that FERPA applies to the HR records of students whose enrollment is a contingency of their employment (TA's, work study awards, etc.) While student data is always student data; Human Resources Data can be both part of the student record and the Human Resources record.
6. **Information Technology Data**—supports the provisioning and management of the technology infrastructure provided by Information Technology Services.
7. **Library and Information Resource Data**—supports the management activities and information resource collection activities of the University libraries, including databases of purchased and locally produced information and digitized files of University archives and other special collections.
8. **Personal Registry Data**—supports the management of identity and authentication for individuals associated with the University, including the creation of unique data elements (such as Banner ID and Student Cards) that provide unambiguous identification and resolution for merging of identity records. Personal registry data can be used to provision other applications that are managing privileges to authorized individuals or groups.
9. **Student Data**—supports all phases of a student's relationship with the University from application through alumni status except as noted elsewhere. This includes, but is not restricted to, demographic data, academic records, disciplinary and medical records, course information, admissions data, housing, and financial aid, as well as employment with the University, which is dependent on student status. Storage, retrieval, destruction, back-up, and data access, among others, to student records are an important part of this policy.

ATTACHMENT 3

DATA GOVERNANCE COMMITTEE

The Data Governance Committee (DGC) is an official University committee that reports to the President of the University and is chair by the University CIO. The DGC will advise the President on the development and enforcement of the University's Data Governance Policy. While the DGC will operate in an advisory role, only the CIO retains the authority to approve and enforce data governance policies, procedures, and standards.

The CIO appoints Committee members. The Committee may include representatives from University Counsel, University Relations, Health Sciences, Strategic Enrollment, Facilities, Provost Office, Labor Relations, Government Relations, Student Life, University Advancement and Foundation, Finance, Information Resources and Technology, the Director of Information Security, and other relevant Senior University Management.

The DGC members or CIO may create subcommittees and task forces as needed to carry out its responsibilities.

Other Committee responsibilities include:

1. **Access** – Defining a single set of procedures for requesting permission to access data elements in University databases, and, in cooperation with Data Stewards, documenting these common data access request procedures.
2. **Conflict Resolution** – Resolving conflicts in the definition of centrally-used administrative data attributes, data policy, and levels of access.
3. **Data Governance** – Establishing policies that manage University Data as a University resource and communicating the policy to the University community.
    - Overseeing the administration and management of all University Data.
    - Resolving issues with regard to standard definitions for data elements that cross stewardship boundaries.
    - Establishing specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation.
    - Identifying data entities and data sources that comprise University Data. As this is an on-going process, the committee will add data entities and sources to the scope of University Data, as circumstances require.
    - Prioritizing the management of University Data. This includes identifying which data is most critical and assigning management priorities to all data entities and sources.
    - Consideration of delivery modes for transmitting University data.

    The DGC, in consultation with University Counsel and the Information Security Office, will also advise on policies related to contracts with vendors whose products or services may process, store, or exchange data with University systems, including third party contracts for secondary systems that share data housed in the University's primary systems such as Banner.
4. **University Data Mode**l – Overseeing the establishment and maintenance of the University Data Model and Data Architecture, which includes defining the standards for documentation of data elements. ?
5. **Shared Data Management** – Defining attributes and assigning maintenance responsibilities for data accuracy, retention, disposition, and preservation. Note that oversight of University data, which is a public record, should be managed according to the Public Records Law and the approved records retention and disposition schedules that are created in University Archives and Records Management Services.

ATTACHMENT 4

DATA STEWARDS

University staffs designated as "Data Stewards" have the primary administrative and management responsibilities for University Data within their functional area. Data Stewards have that role by virtue of their positions. For example, the Sr. Vice President for Human Resources has stewardship responsibility for HR data.

Data Stewards interpret policy, define procedures pertaining to the use and release of the data for which they are responsible, and ensure the feasibility of acting on those procedures. Data Stewards are responsible for defining procedures and policy interpretations for their business; any such business-unit specific items must, at minimum, meet University policy standards. They are responsible for coordinating their work with other

University offices associated with management and security of data, such as University Counsel, the Director of Information Security, and the Division of Information Resources and Technology (IRT). Specific responsibilities include:

1. **Access** – Approving requests for access to data, specifying the appropriate access procedure, ensuring appropriate access rights and permissions according to classification of data.
2. **Communication –** Ensuring that consumers of the data for which the Data Stewards are responsible are aware of information handling procedures.
3. **Compliance** – The Data Steward is ultimately responsible for compliance with applicable University policies, legal and regulatory requirements. Stewards must be knowledgeable about applicable laws and regulations to the extent necessary to carry out the stewardship role. Furthermore, Stewards must take appropriate action if incidents violating any of the above policies or requirements occur.
4. **Consultation** – Providing consulting services as needed to assist data users in the interpretation and use of data elements for which they are responsible, including the Data Custodian.
5. **Coordination** – Ensuring that, where required, Information Security Liaisons are designated for their respective business unit; specifying data management and protections requirements to Data Custodians.
6. **Data Classification** – Classifying each data element according to University definition: Highly Sensitive (high risk), Sensitive (medium risk) and Public (low risk).
7. **Documentation** – Ensuring that documentation exists for each data element to include, at a minimum, the following: data source, data provenance, data element business name, and data element definition.
8. **Data manipulation, extracting, and reporting** – Ensuring proper use of Data and recommending appropriate policies regarding the manipulation or reporting of University Data elements and implementing business unit procedures to carry out these policies.
9. **Data quality, integrity, and correction** – Ensuring the accuracy and quality of data (access and logging controls, backup, etc.) and implementing programs for data quality improvement.
    - Developing procedures for standardizing code values and coordinating maintenance of look-up tables used for University Data.
    - Determining update precedence when multiple sources for data exist.
    - Determining the most reliable source for data. ?
10. **Data lifecycle and retention** – Ensuring appropriate generation, use, retention and disposal, etc. of data and information consistent with University Policies, among them Information Security Policy and standards for disposal. ?
11. **Data stewardship** – Other responsibilities as necessary, including exercise of due care in the selection of Data Custodians to ensure these responsibilities are adequately and consistently executed. ?
12. **Data storage** – Documenting official storage locations and determining archiving and retention requirements for data elements.
13. **Education** – Ensuring that education to employees responsible for managing the data is provided in data retention, data handling and data security.
14. **Policy implementation** – Establishing specific goals, objectives, and procedures to implement the policy and monitor progress toward implementation.

ATTACHMENT 5

DATA CUSTODIANS

Data Stewards may appoint Data Custodians who will assist Stewards with data administration activities. The Data Custodian is given specified responsibilities and receives guidance for appropriate and secure data handling from the Data Stewards. A Data Custodian has the responsibility for the day-to-day maintenance and protection of data.

Specific responsibilities also include:

1. **Access** – Implementing procedures as defined by the DGC and Data Stewards to grant access for Consumers.
2. **Coordination** – With guidance from the respective Data Stewards and in collaboration with technical support staff, Data Custodians recommend appropriate IT procedures that satisfy specified information security requirements, including legal and compliance obligations as well as applicable University policies.
3. **Data collection and maintenance** – Collecting and maintaining complete, accurate, valid and timely data for which they are responsible.
4. **Data security** – Administering and monitoring access and, in collaboration with technical support staff, defining mitigation and recovery procedures; reporting any breaches of University information in a timely manner according to procedures defined in the Incident Management policy; coordinating data protection with the Information Security Office as necessary
5. **Documentation** – Writing the documentation for each data element base upon stewardship requirements, policy, and best practices. This documentation will include, at a minimum, the following: data source, data provenance, data element business name, and data element definition.
6. **Education** – At the direction of the Data Steward, providing education in data retention, data handling and data security to employees responsible for managing the data.