

Data Warehouse Data Policy

Introduction

Administrative data captured and maintained at Rensselaer are a valuable Institute resource. While these data may reside in different database management systems and on different machines, these data in aggregate may be thought of as forming one logical Institute resource. This data warehouse contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision-making.

This policy establishes uniform data management standards and identifies the shared responsibilities for assuring that the data warehouse provides security, protects privacy and has integrity while it efficiently and effectively serves the needs of Rensselaer. This policy applies to those data that are critical to the administration of the Institute regardless of whether the data are used or maintained by administrative or academic units.

Data Security, Privacy, and Access Philosophy

The overarching goal in the data policy is to strike a balance between data access and data security and privacy. The value of data as an institute resource is increased through its widespread and appropriate use; however, its value is diminished through misinterpretation, misuse, or abuse. Of the two concerns, data security and privacy is the more critical and delicate. Access can be expanded as needed, but privacy, once violated, can seldom be repaired and security, once violated, can compromise the financial integrity, reputation, functionality, and stability of the Institute.

As an educational institution with a mission to discover and disseminate knowledge, Rensselaer values accessibility to and the timeliness and accuracy of information while fully appreciating the basic security and privacy requirements involved. However, dissemination of academic or research knowledge (scholarly information) should not be confused with dissemination of information and knowledge used to manage and operate the Institute. This latter class of operational data and information should be readily available within the Institute, albeit on a need-to-know basis. Therefore, permission to view or query data contained in the Data Warehouse should be granted to data users for legitimate purposes. Update access should be restricted as necessary, but granted to Institute employees at the location where data are initially received or originates whenever this is feasible. Permission to view or query data for which there is no justifiable Institute purpose should be denied, and information specifically protected by law or regulation or Institute policy must be rigorously protected from inappropriate access. However, as opportunities and requirements evolve, access permissions must be able to adapt to new circumstances as authorized by data trustees (i.e., President, Cabinet members, or delegated individuals with information accountability).

Policy

Controlled access to administrative information will be provided to employees for the support of institute functions. The breadth and depth of access is determined by the role of the individual and may be contingent upon training on applicable data policies and responsibilities. Security and privacy will be prioritized over access except as required by business need and by formal agreement among the data trustees involved.

Data Management Roles and Responsibilities

President and Cabinet- The President determines overall planning and policy-making responsibilities for Institute data and makes such delegations as deemed appropriate. The Cabinet members, as individuals, are responsible for overseeing the establishment of data management policies and procedures for data governed by their portfolio(s) and for the assignment of data management accountability within

their portfolio(s). These policies, procedures, and accountabilities are to be reviewed by the cabinet as a whole and to be approved by the CIO.

Chief Information Officer (CIO) - The CIO acts as the liaison for the President and the Cabinet to the Institute community and is responsible for overseeing the management of Institute information resources and security. The CIO has signature approval authority for the Data Warehouse policies and procedures.

Data Stewards- These are Institute Directors or above (e.g., the Controller, Registrar, Dean of Enrollment, Director of IACS) who oversee the capture, integrity, maintenance and dissemination of data for a particular operation according to the defined data policies and procedures. Data Stewards perform the data management activities outlined in this policy and share responsibility for data security and privacy with Director levels and above within the CIO organization.

Data Experts- Data Experts are operational managers (e.g., Director of Enrollment Operations, Assistant Registrar) within a functional area with day-to-day responsibilities for managing business processes and establishing business rules for the production transaction systems.

Data Users- Data Users are individuals who access Institute data in order to perform their assigned duties or to fulfill their role in the community. Data users are responsible for protecting their access privileges and for proper use and protection of the data they access. The access policy and any exceptional access privileges are determined by the appropriate Cabinet member for the involved portfolio(s) and are to be reviewed and approved by the CIO.

Data Management Advisory Group- This is a defined Institute-wide group, typically composed of Data Stewards, Data Experts, Data Managers and select Data Users, which reviews the operational effectiveness of data management policies and procedures and makes recommendation to the CIO and Cabinet-level portfolio owners for improvement or change. The group will be chaired by one of its members with the chair responsibility rotated to a different member each year.

Data Integrity, Validation and Correction

Data Stewards are responsible for assuring that the applications that capture and update data incorporate edit and validation checks to protect the integrity of the data.

Data Users are responsible for helping to correct data problems or inaccuracies by supplying as much detailed information as possible about the nature of the erroneous data.

Upon written identification and notification of erroneous data to the Data Stewards, corrective measures should be taken as soon as possible to:

- Correct the cause of the erroneous data.
- Evaluate and appropriately correct the data at the source. (Bad data will not be corrected in the data warehouse. Errors will be corrected in the current period or in the live data, not in prior periods or frozen data snapshots.)
- Notify users who have received or accessed erroneous data.

Approved:

Shirley Ann Jackson

Date