Data Governance & Classification Policy 9.1.1.C - Roles and Responsibilities

Data Trustees

Data Trustees are senior university officials, or their designees, who have planning and policy level responsibility for data within their functional areas and management responsibility for defined segments of institutional data. Data Trustees work with the Chief Information Officer (CIO) to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university.

Data Trustee responsibilities include:

- Assigning and overseeing Data Stewards.
- Overseeing the establishment of data policies in their areas.
- Determining legal and regulatory requirements for data in their areas.
- Promoting appropriate data use and data quality.

Data Stewards

Data Stewards are university officials, or their designees, having direct operational-level responsibility for the management of one or more types of institutional data.

Data Stewards responsibilities include:

- Assisting in developing and maintaining data classification policies.
- Assisting in developing, implementing and managing data access policies.
- Ensuring that data quality and data definition standards are developed and implemented.
- Interpreting and assuring compliance with Federal and State regulations and university policies regarding the release of, responsible use of and access to institutional data.
- Coordinating and resolving stewardship issues and data definitions of data elements that cross multiple functional units.
- Developing, implementing and maintaining a business continuity plan for institutional data under their control. Business continuity is an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses,

maintain viable recovery strategies and plans and ensure the continuity of operations through personnel training, plan testing and maintenance.
- Providing communications and education to Data Users on appropriate use and protection of institutional data.
- Developing, implementing and communicating record retention requirements to the university community in conjunction with University Archives.

Data Steward's with responsibilities that include Restricted data such as social security numbers, must also work with other Data Stewards and Data Custodians with similar responsibilities to:

- Review and approve Restricted data usage and use requests.
- Ensure that individuals with visibility to social security numbers have completed required training and that agreed to confidentiality statements.
- Maintain an updated listing of all supported systems.
- Maintain a listing of data types stored and/or processed.
- Perform periodic reviews to ensure continued compliance with the Data Governance and Classification Policy and all other university policies.

Data Custodians

Data Custodians are central or distributed university units or computer system administrators responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data. Data Custodians must be authorized by the appropriate Data Steward.

Data Custodian responsibilities include:

- Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody.
- Complying with applicable university computer security standards.
- Maintaining disaster recovery plans and facilities appropriate to business needs and adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.
- Managing Data User access as prescribed and authorized by appropriate Data Stewards.
- Following data handling and protection policies and procedures established by appropriate Data Stewards.
- Complying with all Federal and State regulations and university policies applicable to the institutional data in their custody.

Note: University units that develop databases and/or systems from institutional data sources and then provide access to this data to other users are considered Data Custodians. These Data Custodians must be authorized by the appropriate Data Steward, approved to further redistribute institutional data and must implement the minimum required safeguards for the source data as prescribed by the Data Steward.

Data Users

Data Users are university units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university. This access is granted solely for the conduct of university business.
The Data User's responsibilities include:

- Following the policies and procedures established by the appropriate Data Stewards.
- Complying with Federal and State regulations as well as university policies, procedures and standards associated with the institutional data used.
- Using institutional data only as required for the conduct of university business within the scope of employment.
- Implementing safeguards prescribed by appropriate Data Stewards for limited access and Restricted data.
- Ensuring the appropriateness, accuracy and timeliness of institutional data used for conducting university business.
- Reporting any unauthorized access, data misuse, or data quality issues to the IT@UC Office of Information Security and appropriate Data Steward for remediation.

Institutional data covered by this policy include but are not limited to:

Institutional Data Segment Type	Data Trustee
Alumni Relations and Fund Raising	Vice President for Development and Alumni Relations
Equipment and Asset Management Endowment Human Resources (Compensation, Benefits, Payroll)	Senior Vice President for Administration and Finance

Institutional Data Segment Type	Data Trustee
Legal Procurement	Senior Vice President Administration and Finance Vice President General Counsel
Research Administration	Vice President for Research
Counseling Disability Services Student Records Student Admissions Student Financial Aid	Vice President for Student Affairs Vice President for Equity & Inclusion
Budget and Planning Campus Life Construction Facilities and Space Management Financial (General Ledger, Accounts Payable) Student Billing and Accounts	Senior Vice President for Administration and Finance Vice President for Finance Vice President for Student Affairs and Vice President for Equity & Inclusion
Undergraduate and Graduate Student Registration and Graduation Services	Vice President for Student Affairs Vice President for Equity & Inclusion
Student Health	Senior Vice President for Health Affairs Dean of the College of Medicine
Tenure	Vice Provost for Academic Personnel
Learning Management Telecommunication and Networking	Chief Information Officer
FERPA/Student Data	Registrar
PCI, Financial Documents	Treasurer
ISO#, M#	Public Safety
Employee Information (SSN, Address, Personal Contact info, Benefits info, etc.)	Human Resources

Institutional Data Segment Type	Data Trustee
Export Controlled Data: *Any data which cannot be released to foreign nationals or representatives of foreign entities.*	Office of Export Controls
Legal Information	Office of General Counsel

Note: Instances of some data types, for example sensitive personal items such as social security numbers may be covered by multiple Data Trustees depending on the context of collection and use.

Related Links

Data Governance & Classification Policy

Phone Contacts

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 07/01/2009
Revised: 05/30/2014
Revised: 01/25/2017
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019
Revised: 03/03/2022