Trinity University Data Governance Policy

Document Number: ACAD-0014 **Date Published(sys):** 9/8/2026

General Description

Policy Summary:

Trinity's data is a strategic asset, and the efficient use of data is critical to the University's success. It supports the delivery of Trinity's mission of pursuing the highest levels of academic and professional excellence in teaching, research, learning, service, leadership, and personal integrity.

This policy defines an institution-wide framework of principles and decision-making structures and roles for data governance. This framework will enable Trinity to manage its data intentionally and consistently to deliver maximum value in support of its mission.

Successful implementation of this framework will provide a measurable improvement in data security and data usability. It will also enhance the data awareness and capability of those creating, accessing, and using Trinity's data. The demands of information security and mitigating risk will be balanced with the demands of maximizing business value.

This framework is supported by related policies, standards, and guidelines (see Related Documents). These may develop and evolve with the needs of the institution.

Purpose:

The purpose of this policy is to:

- Define roles, responsibilities, and accountability for all parties involved in collecting, using, and disposing of data critical to Trinity University.
- Develop procedures, standards, and processes for effective governance of data.
- 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 Trinity's future information needs.
- Ensure processes are in place to create and maintain data quality.

Scope:

This policy applies to students, faculty, staff, researchers, contractors, visitors, and any others accessing the University's data or computing and network facilities. It applies in all locations where the University conducts its activities without geographical limits, subject to applicable local laws and regulations.

This framework applies to all institutional data owned by the University, under the University's custody, or otherwise present in the University's network or computing environment. This data may be held on any of the University's premises or in any external or cloud-based IT infrastructure licensed, rented or contracted by the University or on the University's behalf. This policy also includes data held on personal devices on the University's behalf.

This policy applies to the governance of institutional data belonging to the University. It does not apply to research data.

Responsible Department:

Academic Affairs

Policy Content

Principles

Data governance is a formal process for making data secure, accurate, and available. It creates an institution-wide framework of principles and decision-making structures and roles. This framework will enable Trinity to manage its data intentionally and consistently to deliver maximum value in support of the institution's mission.

This framework will help Trinity follow data governance processes while upholding the following principles:

Data is a valued asset.

- Data has value as much as other assets such as buildings, vehicles, or money.
- Like other university assets, institutional data does not "belong" to individuals or units. Instead, it is managed by them on behalf of the university.
- Data shall be identified and defined so that its value can be leveraged and it can be managed appropriately.

Data is managed.

- Data shall be appropriately managed (i.e., collected, stored, protected and used) throughout its life cycle.

- Data management shall be a core capability that is an integral part of the University's culture.
- Named roles with specific responsibilities across the data lifecycle, from data entry to archive or disposal, should be defined, trained, and appropriately resourced.
- The single, master source for each different type of data shall be identified and data systems and integrations structured to rely on that source.

Data is fit for purpose.

- Data shall be accurate and complete, at the appropriate quality for its primary purpose and all other known legitimate uses.
- Data shall be monitored so it can be trusted. Data stewards have the role of accountability and oversight to assure this trust, with decisions and actions recorded at an appropriate level of detail.

Data is accessible, comparable and reusable

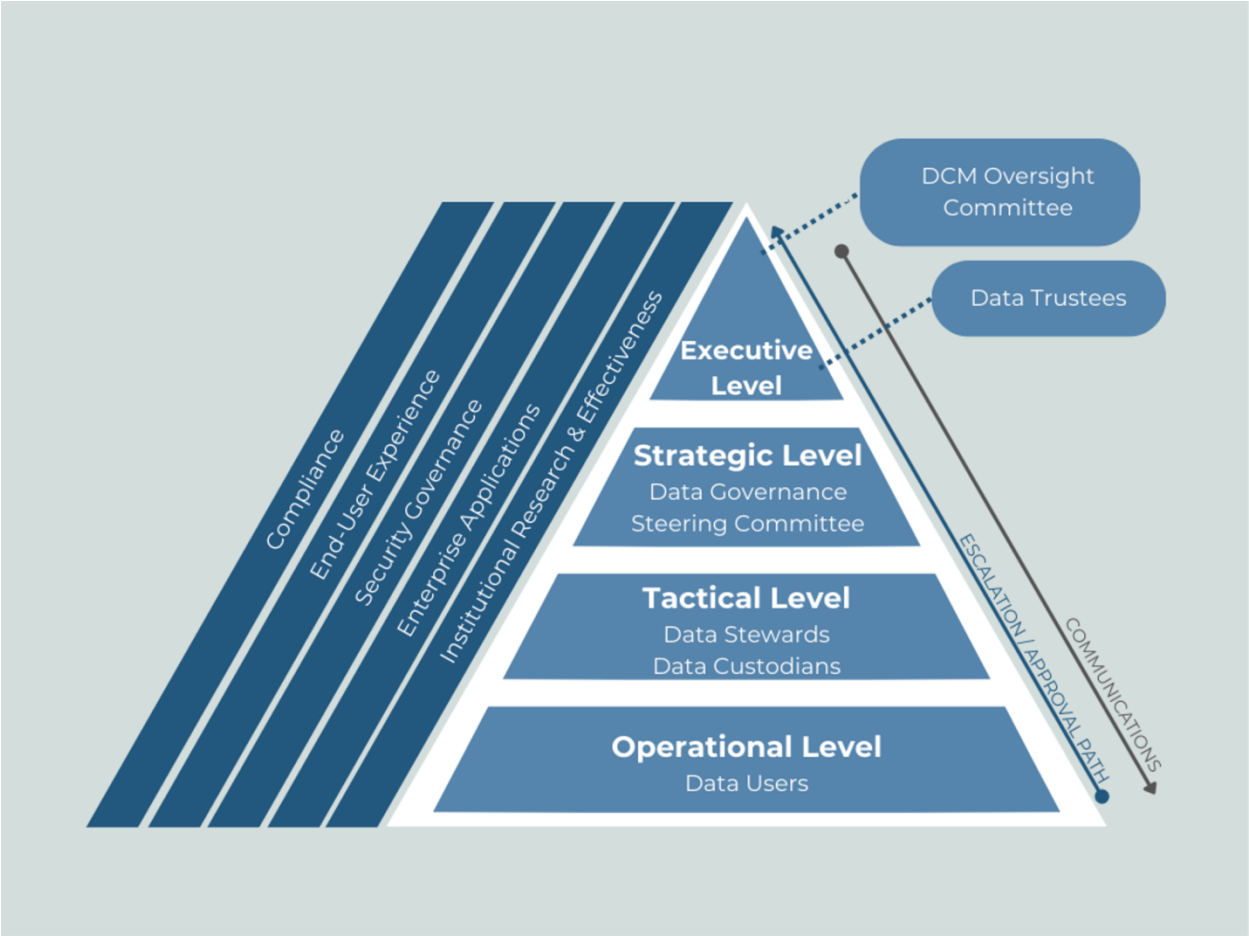
- Data access rules shall be clearly defined so that it can be made available where and when required, subject to appropriate security constraints.
- Standards will be consistently applied to encourage reuse, and promote a common understanding of context, meaning, and comparability.
- Data shall be easy to find, quick to understand, and simple to compare.
- Data shall be consistent and predictable, avoiding harm caused by conflicting versions.

Data is secure and compliant with regulations.

- Data shall be protected against unwanted, or unauthorized access. Appropriate confidentiality shall be maintained.
- Data shall be acquired, used, stored and disposed of in compliance with the law and applicable standards, regulations and contractual obligations.
- Data integrity protects the university from reputational, financial, and regulatory damage.

Roles and Responsibilities

The activities of data governance are applying policies, standards, guidelines, and tools to manage the institution's data. Responsibility for the activities of data governance is shared among the roles listed below. Descriptions of roles and responsibilities below provide the framework of how data governance should be implemented and maintained.



Executive Level

The executive level, which includes the Digital Campus Management Oversight Committee and Data Trustees, is responsible for ensuring that data governance is implemented and has sufficient resources to succeed, including actively promoting data governance practices at Trinity University.

Digital Campus Management (DCM) Oversight Committee

The DCM Oversight Committee provides oversight of data governance as well as other aspects of the digital campus. This structure facilitates coordination across multiple areas of digital campus management, including:

- Enterprise Applications
- Security Governance

- Data Governance
- End-User Experience

The DCM Oversight Committee is responsible for:

- Approving data governance strategy
- Approving data governance related documents such as a data role framework, data policies, and data governance priorities, methods, and tools
- Reporting on data governance activities to the CEO and Board of Trustees
- Providing resources for data quality remediation

Data Trustees

Data Trustees are executives who are responsible for:

- Collaborating with the Chief Information Officer to ensure that appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the university
- Appointing a data steward for each domain/subdomain in their division
- Promoting data governance practices within their divisions
- Supporting cross-unit data governance priorities

Strategic Level

The strategic level, which includes the Data Governance Steering Committee and the Chief Data Officer (CDO), is responsible for setting the strategic direction and overseeing the implementation of data governance at Trinity University.

Data Governance Steering Committee

The Data Governance Steering Committee is comprised of the Chief Data Officer (CDO), the Director of Enterprise Applications and Architecture, the Data Stewards for each of the core data domains, and a faculty representative of the Educational Review and Technology Committee (ERTC). It is responsible for the following tasks:

- Developing data governance strategy
- Developing data governance related documents such as a data role framework, data policies, and data governance priorities, methods, and tools
- Overseeing the implementation and maintenance of the data governance strategy, policies, and tools
- Assigning each asset and system to the appropriate data domain

- Monitoring the effectiveness of the data governance framework
- Making recommendations for improvement to the data governance framework
- Sponsoring education and training for employees on data governance
- Reviewing Faculty Handbook language and suggesting revisions to the Faculty Senate to match policy recommendations

Chief Data Officer

The Chief Data Officer (CDO) is responsible for supporting data governance tasks, including:

- Chairing the Data Governance Steering Committee and taking a lead role in accomplishing its responsibilities
- Developing methods for assessing the effectiveness of data governance practices, including data documentation, data quality, and compliance

Tactical Level

Data Stewards

Data Stewards are university officials, or their designees, who are identified by Data Trustees as having direct operational-level responsibility for the management of one or more domains or subdomains of institutional data.
With the assistance of the Chief Data Officer, their tasks include:

- Serving on the Data Governance Steering Committee (data stewards of core domains only)
- Attending monthly Data Stewardship Committee Meetings or sending a delegate (depending on the domain, stewards of some functional domains are optional unless requested)
- Identifying Data Custodians for each of the domains or subdomains for which they are responsible

Policy Review and Enforcement

- Recommending policies to the Data Governance Steering Committee and providing feedback on draft policies
- Establishing procedures and guidelines to implement data governance policies (concerning data access, completeness, accuracy, privacy, and integrity) for the domains or subdomains for which they are responsible

- Performing periodic reviews to ensure continued compliance with data protection and classification policies and all other university policies that pertain to data in the domains or subdomains to which they are assigned

Regulatory Compliance

- Defining who can access and use data in the domains or subdomains to which they are assigned, including reviewing restricted data usage and use requests
- Determining legal and regulatory requirements for data in their areas, in collaboration with the Chief Compliance Officer
- Developing, implementing, and communicating record retention requirements
- Ensuring that individuals with visibility into protected data have completed required training and have signed confidentiality agreements

Data Documentation

- Creating a data catalog of the assets/systems under their purview and data dictionaries describing what is in them
- Documenting metadata, including the source of data assets and their contents
- Identifying critical data elements (CDEs)
- Creating a business glossary of business definitions for CDEs

Data Quality

- Defining the data quality rules for each CDE
- Enabling CDEs for data quality monitoring (i.e., creating methods for ensuring that CDEs are high quality across all data quality dimensions)
- Identifying data quality issues and creating plans to address them
- Publishing data quality KPIs and data quality remediation scorecards to the Steering Committee

Data Custodians

Data Custodians are computer system administrators responsible for the operation and management of systems and servers that collect, manage, and provide access to institutional data. Data Custodians must be authorized by the appropriate Data Steward.
Under the direction of the Data Steward, their tasks include:

- Following the procedures and guidelines established by Data Stewards to implement data governance policies
- Monitoring data quality

- Supporting users in understanding and using data correctly
- Provisioning, modifying, and deprovisioning least-privilege, role-based access to systems and applications as authorized by the Data Steward, if applicable, and logging/monitoring access to restricted/confidential data

Operational Level

Data Users

Data users are individuals who are authorized to receive, process, or otherwise handle data to fulfill business responsibilities. Their role in data governance is observing all relevant data governance policies and standards.

Other Roles that Impact Data Governance

Department Managers

Department Managers are responsible for defining employee responsibilities, managing day-to-day operations of their group, and requesting user access.
Their role in data governance includes:

- Requesting data user access through ITSupport@trinity.edu or the appropriate system administrator
- Notifying Human Resources of employee rights changes and/or terminations
- Completing role-specific training to enhance data literacy and acceptable data use

Human Resources

Human Resources serves as a central point of contact for defining organizational roles and profiles, notifying ITS and data stewards of termination or role change, and addressing non-compliant workforce members.
Their role in data governance includes:

- Ensuring that ITS and relevant Data Stewards are promptly notified of employee or contractor terminations, department transfers, and pending terminations
- Determining sanctions for policy violations

Decision Authority and Escalation

Data governance decisions shall be made at the appropriate level to ensure consistency, accountability, and alignment with institutional priorities.

Data Stewards have authority to make operational decisions within their assigned domains or subdomains, including data definitions, data quality rules, access approvals consistent with policy, and metadata documentation.

The Data Governance Steering Committee has authority to resolve conflicts that span multiple domains, approve enterprise data standards, and interpret this policy where ambiguity exists.
Data Trustees and the Digital Campus Management Oversight Committee have final authority for decisions with significant institutional risk, regulatory impact, or resource implications.

Issues that cannot be resolved at the steward level shall be escalated to the Data Governance Steering Committee. Issues that remain unresolved or that present material institutional risk shall be escalated to the executive level for final determination.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Data Governance	Data governance is the practice of formalizing behavior around the availability, usability, integrity, and security of data. It includes establishing roles and responsibilities for data access, definition, and quality to enable Trinity to use data effectively while ensuring security and confidentiality.
Data	Data is a collection of facts, numbers, words, observations, or other useful information. It can be structured (i.e., organized in a clear, predefined format) like data tables with rows and columns or unstructured (i.e., not organized in a predefined format) like PDFs of transcripts stored in folders.
Data Lifecycle	A data lifecycle represents all the life stages of data, including collecting/creating, storing/maintaining, using/processing, sharing/disseminating, and archiving, and/or destroying/purging data.
Data Domain	A data domain is a broad category of data that is managed as a group. Each data domain

Term:	Definition:
	includes related types of data that are tied to a business function.
Data Subdomain	Data subdomains are smaller, more specific categories within a data domain. These subdomains represent finer divisions of data that correspond to particular business processes or areas of activity within the broader domain.
Core Domain	Core domains impact multiple functional areas, are important for institution-level planning, use shared resources, and are essential for ensuring consistency and integration across systems.
Functional Domain	Functional domains are more localized than core domains both in their management and in their impact.
Data Catalog	An inventory of Trinity's data assets that provides an overview of all available data. Helps data users find the data they need.
Data Dictionary	Defines the data in a data asset. Includes information about how to describe or manage data, rather than the data itself. Helps users understand the types of data in a data asset and their meaning.
Business Glossary	A glossary of business definitions (see below) to help users understand Trinity's Critical Data Elements (see below)
Business Definition	A clear and concise description of a data element that helps drive understanding of the meaning of data.
Critical Data Element (CDE)	Data that informs and enables Trinity's operations, decision-making processes, risk management, reporting accuracy, and compliance with regulatory requirements.
Data Quality	Describes the accuracy, completeness, consistency, validity, timeliness, uniqueness, and integrity of data (see below).
Metadata	Data that describes information about other

Term:	Definition:
	data, including business metadata, operational metadata, and technical metadata.
Business Metadata	Metadata that connects data domains to data stewards, drives business data definitions, and supports compliance by connecting data with security classifications, retention policies, and data regulations.
Operational Metadata	Metadata that contains information about how and when the data was created or transformed. It may include information such as time stamps, location, or job execution logs.
Technical Metadata	Metadata that shows where data came from in terms of the physical databases, systems, and data flows across the institution. Technical metadata also describes data structure, storage, format, and processing. This type of metadata usually includes information such as data types, column names, and table structures.
Accuracy	Free from error; reflects reality
Completeness	Includes all necessary parts; no missing information
Consistency	Aligns with other data as expected
Validity	Conforms to predetermined format and constraints
Timeliness	Current; available when needed
Uniqueness	Unique; no duplication in records

Related Documents

Related Documents:

Document Type:	Document Name:	Document Number:
Policy	Family Educational Rights & Privacy Act	REGR-0001
Policy	Records Retention Policy	GNCL-0003
Policy	Incident Response Policy	ITS-0012
Policy	Information Security Policy	ITS-0013
Policy	Access Control Key Policy	EMAC-0003
Policy	Physical Security for Technology Rooms Policy	ITS-0018
Policy	Social Media Policy	SCM-0001
Policy	Student Accessibility Services Confidentiality Policy	ACSP-0001
Policy	Rights, Responsibilities & Privacy	FINA-0005
Policy	Password Policy	ITS-0015
Policy	Data Protection Privacy Notice - General Data Protection Regulation (GDPR)	ITS-0021

Related Content:

This list of regulations is subject to change as new regulations emerge or as referenced website links change.

Federal Data Regulations
Family Educational Rights and Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)

International Data Regulations
General Data Protection Regulation (GDPR)

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v1	7/27/2026 1:41 PM	Pamela Mota

Vice President Approval:

Name:	Title:
Megan Mustain	Provost and Vice President for Academic Affairs