# UTAH VALLEY UNIVERSITY
Policies and Procedures

| | | | |
|---|---|---|---|
| **POLICY TITLE** | Institutional Data Governance and Management | **Policy Number** | 445 |
| **Section** | Facilities, Operations, and Information Technology | **Approval Date** | March 28, 2024 |
| **Subsection** | Digital Transformation | **Effective Date** | March 28, 2024 |
| **Responsible Office** | Office of the Vice President of Digital Transformation | | |

## 1.0 PURPOSE

**1.1** Information owned and maintained by the University is a vital asset that employees and students use to support the University's mission and operational needs. The University has a responsibility to preserve and protect these assets. The University also has a responsibility to provide access to those who need information assets for the performance of their administrative or academic duties, strategic planning, and other official responsibilities that support the University's educational mission.

**1.2** This policy establishes the University's data governance rules and procedures and defines the University's data management function. Together, effective data governance and data management ensure that the University uses this vital asset to make data-informed decisions while managing institutional risk.

## 2.0 REFERENCES

**2.1** *Student Rights and Responsibilities,* Utah Code Ann., §53b-28-503(2022)

**2.2** Utah Board of Higher Education Policy R345 *Information Technology Resource Security*

**2.3** UVU Policy 132 *Institutional Data Collection and Research*

**2.4** UVU Policy 133 *Compliance with Government Records Access and Management Act*

**2.5** UVU Policy 136 *Intellectual Property*

**2.6** UVU Policy 138 *Institutional Review Board*

**2.7** UVU Policy 207 *Internal Audit*

**2.8** UVU Policy 447 *Information Security*

**2.9** UVU Policy 449 *Private Sensitive Information*

**2.10** UVU Policy 451 *Retention of Electronic Files*

**2.11** UVU Policy 457 *PCI DSS Compliance*

**2.12** UVU Policy 542 *FERPA (Student Records Act)*

**2.13** UVU Policy 548 *Academic Rights and Responsibilities of Healthcare and Counseling Clinical Program Students*

**2.14** UVU Policy 710 *Clery Act Compliance*

## 3.0 DEFINITIONS

**3.1 Access:** For the purposes of this policy, a user's ability to read or view institutional data. Access does not include the ability to create or modify data.

**3.2 Data analyst:** A person who analyzes data to support the University's mission or administrative processes.

**3.3 Data classification**: Groupings used to define levels of data sensitivity and identify the level of protection the data requires.

**3.4 Data consumer**: Any person who has access or requests access to institutional data or information.

**3.5 Data context**: Contextual characteristics of institutional data including but not limited to the data domain or subdomain, the organization to which the data applies, or the basis on which job or other functions are assigned (e.g., level of position, position classification).

**3.6 Data custodian**: Subject matter expert for technical definitions, systems, data sets, or access protocols for a data domain or sub-domain.

**3.7 Data domain or subdomain**: A grouping of data and information related to a cabinet-level segment of operational processes and systems. Areas of expertise, accountability, and processes may be segmented within a domain.

**3.8 Data governance**: The processes associated with describing and classifying data and rules for data access so data can be used, trusted, and securely and appropriately shared.

**3.9 Data governance role**: An institutional role performed by an employee with the requisite knowledge of the subject matter, authority to make decisions related to that subject matter, and accountability for the business or technical processes related to data.

**3.10 Data governance standard**: A standard or rule that is relevant to the data within at least one data domain (or subdomain). It is based on policy or law and further explains how the University interprets the policy or law. It may also name or require the documentation of procedures that describe how the interpretation is applied.

**3.11 Data governance system**: A software system that is used to create, maintain, and share metadata related to the University's data, data systems, and the information derived therefrom. It is also used to perform data governance tasks (e.g., managing requests for access or creating new system codes).

**3.12 Data infrastructure**: The physical technology architecture and digital systems that contain information critical to the success of the University.

**3.13 Data management**: The administration and application of digital systems and technologies for the storage and use of data so it can be used, trusted, and safely shared.

**3.14 Data owners**: Chief executives or vice presidents who have strategic planning and policy-level responsibility for their divisions.

**3.15 Data persona**: The combination of attributes that apply to a data consumer that are used by a data steward to determine the availability of institutional data.

**3.16 Data retention**: The method and length of time data or information is stored by the University.

**3.17 Data steward**: Subject matter expert for the business processes, policies, laws, and data within a specific data domain or sub-domain.

**3.18 Data technician**: An individual who has job responsibilities related to data entry and data transactions.

**3.19 Data trustees**: An executive who holds a position of control and accountability for a data domain or subdomain.

**3.20 Digital systems**: Systems designed to store, process, and communicate information in digital form.

**3.21 Enterprise Architecture Guidelines**: A set of guidelines that outline the University's technology architecture philosophy, requirements, and development and integration standards. The guidelines promote agile development of digital solutions for users and follow a set standard of structure and content (e.g., *The Open Group Architecture Format*).

**3.22 Information asset**: Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the University to perform its business functions.

**3.23 Institutional data**: Any data or information (in any form, location, or unit) that satisfies one or more of the following criteria (institutional data does not include personal medical, psychiatric, or psychological data for both employees and students; data created or used in the conduct of research; or information created through acceptable, limited personal use of university systems that is not related directly to university functions):

**3.23.1** Data created, received, maintained, or transmitted by or on behalf of the University in the management and operation of educational, clinical, research, or business activities. This includes data that are used for analysis to guide and inform the strategic priorities of the University or that are substantive, reliable, and relevant to the management and operation of the University.

**3.23.2** Data that the University is required to maintain or ensure the integrity of by federal or state law, or other compulsory policy or formalized agreement.

**3.23.3** Data required to ensure accurate technology integrations for the smooth functioning of university digital systems.

**3.23.4** Data that are used to derive any data element that meets the above criteria.

**3.24 Specialty data systems**: Locally controlled and managed systems without enterprise integration that may be necessary or required for the institution to carry out obligations related to a grant, contract, or other stakeholder interest that is specialized in nature and is related to obligations, which may or may not integrate with other external enterprise systems at the local, regional, or federal level.

## 4.0 POLICY

### 4.1 Policy Statement

**4.1.1** In accordance with industry best practices and data governance principles, the University shall determine levels of access to institutional data. The University complies with state and federal law by restricting access to certain types of information.

**4.1.2** The University expressly forbids the use of institutional data for anything but the conduct of university business.

**4.1.3** Individuals who access data must observe requirements for confidentiality and privacy and must comply with university protection and control procedures as documented in university policies and related procedures. Employees who present data for research, educational, institutional planning purposes, or any other use must accurately present the data.

**4.1.4** Data consumers are responsible for completing the required training on the appropriate use and protection of university information assets. Data consumers' failure to complete the required

training or protect the University's information assets may result in them losing access to data and/or being subject to other university sanctions.

**4.1.5** Access and protection of data for the purposes of research related to human subjects is specifically governed by Policy 138 *Institutional Review Board*. This policy (Policy 445) does not override Policy 138.

**4.2 Data Infrastructure**

**4.2.1** The infrastructure and management of institutional data shall be based on the University's *Enterprise Architecture Guidelines*. These guidelines and data definitions will be referenced in the University's data governance management system. The Chief Information Officer is responsible for ensuring the *Enterprise Architecture Guidelines* are defined, maintained, and made available to university partners and employees who are responsible for data management and other digital technology development and support functions. These individuals and entities shall adhere to the guidelines.

**4.2.2** Digital Transformation (Dx) shall implement and manage a data governance system. The data governance system shall support the management of governance artifacts, data dictionaries, and a data catalog; data profiling and categorization for accurate classification by data stewards; and automation integration for appropriate access permissions.

**4.3 Data Governance Organization, Roles, and Responsibilities**

**4.3.1 Data Governance Council ("the Council").** The University's data governance organization model includes an executive committee—the Data Governance Council—and named roles with specific responsibilities within a data domain or subdomain: data owners, data trustees, data stewards, data custodians, and data technicians.

**4.3.2 Data owners.** Data owners are accountable for data trustworthiness, security, and privacy within their purview. They support university data governance through the assignment of data governance roles and responsibilities within their division.

**4.3.3 Data trustees.** Data trustees oversee the work of data governance within their domain or subdomain and have the right to act on behalf of the data owner within their data subdomain. Data trustees serve on the Council. Data trustees provide support to the data steward(s) in their area to ensure they can carry out their responsibilities for data quality and appropriate access through business process improvement. In rare circumstances when an executive is not available to serve as a data trustee, the data owner may assign this role to another employee.

**4.3.4 Data stewards.** Data stewards are responsible for daily governance activities including managing and protecting the data and ensuring the accuracy and quality of data within a data domain or subdomain. These responsibilities include classifying data; determining and documenting the data personas that may access the data; approval, documentation, and

implementation of new data codes required by digital systems; assisting with the assessment of university data governance effectiveness; and defining operational needs for data capture within university data systems, including the storage of data based on date/time frequency or key dates and processes. It is recommended that data stewards do not serve as data trustees or vice versa. In some data domains, the availability of positions to fill data governance roles may warrant an exception to this recommendation, which must be approved by the data owner.

**4.3.5 Data custodians.** Data custodian responsibilities include supporting the data steward by creating and maintaining metadata artifacts such as a data dictionary or business glossary and documenting the relationship between information assets and metadata artifacts or entries in the university data governance system. They contribute to the university's data catalog by developing and/or validating stored procedures, queries, or business intelligence assets that can reliably be used by data consumers.

**4.3.6 Data technicians.** Data technicians have job responsibilities that involve data entry and data transactions that modify the information within a given data set or enterprise system.

**4.4 Data Governance Council Membership and Responsibilities**

**4.4.1** The Council membership consists of individuals who have planning and policy-level responsibilities for university operations within their functional areas. The Council shall include at least one institutional data trustee from each data domain as appointed by the data owner and representation for the following areas and roles:

**4.4.1.1** Digital Transformation Division, Data Management Portfolio

**4.4.1.2** Digital Transformation Division, Executive Leadership

**4.4.1.3** Digital Transformation Division, Enterprise Architecture

**4.4.1.4** University FERPA Officer/University Registrar

**4.4.1.5** Faculty Senate President or designee

**4.4.1.6** Chief Engagement and Effectiveness Officer

**4.4.1.7** Office of General Counsel, Risk Management

**4.4.1.8** Government Records Access Management Act (GRAMA) Officer

**4.4.2** A data trustee who also has responsibility in one of the above areas may serve on the Council representing dual roles.

**4.4.3** The Council shall establish and maintain a council charter. This charter shall document the specific responsibilities of the Council.

**4.4.4** The Council develops and oversees the creation, implementation, and assessment of the data governance plan. The Council is also tasked with ensuring the plan is published and available to the university community and appropriate stakeholders.

**4.5 Data Classification**

**4.5.1** All university data and any information derived from it shall be classified in one of the following categories of sensitivity:

**4.5.2 Restricted**

**4.5.2.1** Restricted data is information that, if made available to persons without appropriate authority or accountability, poses a significant risk to the University and its mission. Such data is made available only to those who have a need related to the performance and accountability of their position with the University or who are approved through the University's data governance procedures.

**4.5.2.2** Restricted data may include content such as legal proceedings or documentation related to internal appeals processes, data elements restricted by law or policy such as Social Security numbers, PCI data, or detailed personnel files and evaluations.

**4.5.3 Confidential**

**4.5.3.1** Confidential data is information that is not generally available to the public and that the University has identified as confidential, that should reasonably be understood to be confidential, or that university is obligated to keep confidential under applicable laws, regulations, contractual obligations, university policies, or the policies of relevant government agencies. This includes but is not limited to PII, student records, financial information, research data, and sensitive information. This data is made available only to university employees who have a need to know the information to perform their job duties. These duties, for example, might be making operational or strategic decisions within their purview, preparing reports, ensuring data quality, processing operational transactions, or communicating with specific student or employee populations.

**4.5.3.2** Confidential data may include content such as student or employee demographics (e.g., ethnicity and race, gender, age, or birthdate), formal advising notes, legal contracts or procurement agreements.

**4.5.4 Internal**

**4.5.4.1** Internal data is information that is available only to university employees or entities who have a contractual obligation to protect the data.

**4.5.4.2** Internal data may include student enrollment information, course enrollment counts, outreach and marketing lists, strategic planning documents, employee position information, and institutional SRI results aggregated by college or department.

**4.5.5 Public**

**4.5.5.1** Public data is data or information that is broadly available to the University community and general public.

**4.5.5.2** Public data may include content such as university press releases, institutional fact books or published statistics, campus maps, a UVU catalog, and approved university policies.

**4.6 Data Context**

**4.6.1** Data context may be used as another characteristic dimension, in conjunction with data consumer personas, to identify appropriate access levels for individual data consumers. Wherever possible, data management strategies and systems should be deployed that perform assignment and removal of these access levels systematically when the contextual characteristics of an individual change (e.g., change of assignment, new department, change in employment status).

**4.7 Access to Institutional Data**

**4.7.1** The University may, at any time, revoke access to institutional data based on evidence of behavior contrary to policy or law. It may also temporarily suspend access if there is reasonable suspicion that a data consumer has put the institution at risk, whether willfully or not.

**4.8 Data Consumers**

**4.8.1** Institutional data access is granted based on an individual data consumer's data persona. The data steward determines the specific data personas that should have access to data within their data domain based on factors such as data context and classification.

**4.8.2** Data management processes shall be implemented to ensure that when a data consumer's persona changes, their access to any institutional data is appropriately changed, whether through system automation or manual procedures.

**4.8.3** Data consumers who access data for analysis or presentation to other parties are responsible for the accurate presentation of that data.

**4.8.4** Data stewards support data consumers by creating common business terms, data definitions, and other artifacts and by reviewing and approving the publication of data sets or other business intelligence assets.

**4.8.5** Data analysts shall follow university standards for the development of business intelligence assets such as dashboards or data sets. This includes following data visualization guidelines wherever possible and reasonable to promote data literacy and accurate representation.

### 4.9 System Integration

**4.9.1** Data sharing between institutional systems and external systems not managed by the University, or a combination thereof, will be governed and managed through data classifications and other governance information documented by data stewards in the University's data governance system, following *Enterprise Architecture Guidelines* and guidance from the Office of General Counsel.

## 5.0 PROCEDURES

| POLICY HISTORY | | |
|---|---|---|
| Date of Last Action | Action Taken | Authorizing Entity |
| October 14, 2004 | Policy approved. | UVU Board of Trustees |
| March 28, 2024 | Revised policy approved. | UVU Board of Trustees |