# TEMPLE UNIVERSITY

**Title:** Data Usage, Governance and Integrity Policy
**Policy Number:** 04.71.10
**Issuing Authority:** Office of the President
**Responsible Officer:** Provost

**Date Created:** October 14, 2019
**Date Last Amended/Reviewed: N/A**
**Date Scheduled for Review:** August 2024
**Reviewing Office:** Office of Information Technology Services

## I. Purpose

This Policy provides a framework intended to: (1) promote the establishment, maintenance and expansion of trustworthy, stable, reliable, secure, confidential, and accessible collections of Institutional Data (as defined below); (2) maximize the value derived from Institutional Data by increasing the understanding and use of such data; (3) ensure access to Institutional Data in accordance with institutional policies, and international, federal, state and local privacy and security laws and regulations; and (4) facilitate the use of data as an integral part of decision-making and delivery of services.

## II. Data Definitions

A. **Data** means all facts, measurements, or statistics used as a basis for reasoning, discussion, or calculations.

B. **Institutional Data** means any Data which:
   i. is created, received, maintained, transmitted or reported as a result of the university's educational, administrative, research, creative, service or clinical activities[1]; or
   ii. is used to derive or develop Institutional Data; or
   iii. is generated by a Data User (as defined below) using any of the above Data.

C. **Data Integrity** means the accuracy, availability, completeness, consistency and reliability of Institutional Data. More specifically:
   i. ACCURACY means that Institutional Data is entered and maintained in a manner intended to ensure the data is free from errors.
   ii. AVAILABILITY means that Institutional Data is made available through user-friendly systems intended to ensure timely access and transparency to authorized users.

[1] Subject to applicable university policies pertaining to academic freedom and ownership of scholarly or creative work, a faculty member has the right and authority to control the appropriate use of, and access to, any data arising from research or creative work.

iii. COMPLETENESS means that all reasonable efforts are used to ensure that all available values are present in Institutional Data.
iv. CONSISTENCY means that Institutional Data satisfies a set of definitions or constraints that are applied and maintained uniformly across reports.
v. RELIABILITY means that independent custodians or users are able to obtain consistent results when applying the same definitions or constraints to Institutional Data.

## III. Data Classifications

Institutional Data at Temple University is classified into the categories below. Further detail and examples of these classifications can be found in Information Technology Services' Data Classification, which can be found at http://its.temple.edu/data-classifications.

A. **Confidential Data** is Institutional Data the unauthorized disclosure of which may have a serious adverse effect on the university's business relationships, operations, reputation, resources, services, or constituents. Confidential Data is protected under international, federal, state or local regulations, as well as under institutional policies and contractual obligations.

B. **Sensitive Data** is Institutional Data the unauthorized disclosure of which may have a moderate adverse effect on the university's business relationships, operations, reputation, resources, services, or constituents. Institutional Data is presumed to be Sensitive Data when there is no information indicating that such Institutional Data should be classified as either Confidential or Public.

C. **Public Data** is Institutional Data the disclosure of which poses little or no risk to the university's business relationships, operations, reputation, resources, services, or constituents. Public Data includes Institutional Data that the university publishes in compliance with regulatory and similar requirements.

## IV. Data Governance Principles

The following principles are the core of Temple's approach to data governance:

A. **Data is an asset.** Institutional Data is a valuable asset supporting, among other things, timely and informed decision-making, and is managed accordingly. It is not owned by a particular individual, unit, department, or system of the university. Repositories and usage of Institutional Data are managed by

individuals in assigned roles using stewardship principles that support institutional goals and objectives.

B. **Data must be defined.** Institutional Data must be defined consistently throughout the institution using common vocabulary and definitions, and these definitions must be available and understandable. A common vocabulary facilitates communications and enables dialogue, both among users and systems.

C. **Data must have integrity.** Explicit criteria to ensure Data Integrity must be established and promoted.

D. **Data must be properly secured.** In accordance with institutional policies and international, federal, and state laws, Institutional Data must be protected from deliberate, unintentional or unauthorized alteration or destruction and from inappropriate disclosure or use.

E. **Data must be accessible**. In order to derive the maximum value from Institutional Data, it must be shared across institutional functions and organizations and authorized users provided access necessary to perform their duties. Authorization to access Institutional Data, including confidential and sensitive data, is based on appropriateness to the user's role and the intended use. Authorization and access is granted, documented, reviewed, modified, and terminated in accordance with university policies and international, federal and state laws. Appropriate access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery.

## V. Data Stewardship Roles and Responsibilities

**Overview.** Temple University maintains a role-based governance model for Institutional Data. Authorization to access Institutional Data within these roles is based on applicable law, appropriateness to the user's role, and the intended use. The roles are as follows:

A. The **Executive Data Council** (EDC) is the highest-level data administrative body at Temple University. The Executive Data Council defines the strategy and resolves questions related to data and information management across the organization. The Executive Data Council is comprised of the Vice President, Information Technology Services and such other persons as are designated by the President from time to time. The Executive Data Council:
   i. Defines clear data principles and guidelines for the institution;
   ii. Sets priorities that address relevant, mission critical needs of the university;

iii. Resolves questions regarding appropriate use of Institutional Data and mediates any disputes that may arise;
iv. Promotes data management and security training, education and awareness.

B. The **Operational Data Council** (ODC) is a made up of Data Managers and data experts from across the campus. The Operational Data Council:
   i. Develops procedures and practices to ensure data integrity;
   ii. Develops and maintains the Data Dictionary;
   iii. Identifies data expertise across the university;
   iv. Provides educational forums for Data Managers and users.

C. **Data Officers** are university officials with policy-level responsibility for managing a major area of the university's information resources. Data Officers are designated by the Information Technology Services, subject to consultation and approval of the Executive Data Council (as described above). Data Officers are responsible for designating Data Stewards and assigning data management roles for their units. Data Officers reinforce the importance of Data Integrity and create an environment in which Data Users are encouraged to use Institutional Data correctly, and to identify and correct inaccurate, inconsistent or unreliable data.

D. **Data Stewards** are university officials with policy-level responsibility that have been designated by a Data Officer to serve as the delegated authority for a specific unit. Data Stewards determine access to Institutional Data in the unit, create and manage processes to ensure Data Integrity, and implement appropriate controls for access to and use of Institutional Data. Data Stewards designate Data Managers for their unit.

E. **Data Managers** are university officials that have operational-level responsibility for the capture, maintenance and management of Institutional Data for specific areas. Data Managers must ensure that procedures are in place to carry out policies and comply with university standards.

F. **Data Users** are individuals who have been properly granted access to Institutional Data or the university's information technology systems. This includes university departments, individual university community members, or university affiliates that have been granted access to Institutional Data in order to provide services to the university or to otherwise conduct university business.

G. **Data Management Integration Coordinators** are university staff who are responsible for facilitating and resolving management issues with respect to Institutional Data. Data Management Integration Coordinators train Data Managers and Data Users in the structure, definitions and use of Institutional

Data, and also facilitate the development and documentation of definitions of commonly used data terms.

**VI. Intentional falsification; Security Breaches; Misreporting; No Personal Use.**
Institutional Data must be safeguarded to maintain the confidentiality and privacy of personally identifiable information and must be protected against misreporting, systematic errors, loss, and security breaches, in accordance with applicable law and university policy. Temple prohibits all who work with Institutional Data from knowingly falsifying, fabricating or altering Institutional Data or destroying or deleting Institutional Data unless such data is subject to destruction or deletion under applicable records retention rules or applicable law. Personal use of Institutional Data is prohibited. Data Users must promptly report inaccurate, inconsistent or unreliable data to the appropriate Data Steward or anonymously through Temple's Ethics & Compliance Helpline at https://www.temple.edu/about/ethics-compliance/helpline.

**VII. Research Data and Information**
This policy must be read in conjunction with university policy regarding research data and information ("Research Data Policy"). In the event of any conflict between a Research Data Policy and the provisions hereof with respect to Research Data and Information, the terms of a Research Data Policy shall govern.

**VIII. Data Rules**
The university maintains, and may from time to time update or revise its *Data Rules* relating to the use of and access to specific types of Institutional Data and Temple's electronic resources. The *Data Rules* are maintained by the Vice President, Information Technology Services, in consultation with the Executive Data Council and Operational Data Council, and are available on the Information Technology Services web site.

**Notes**

1. **Dates of official enactment and amendments**

   Adopted by the President on October 14, 2019.

2. **History** N/A

3. **Supersedes**

   This policy supersedes and replaces the following policies and guidelines, which are hereby rescinded:

Social Security Number Usage Policy, policy number 04.75.11, adopted by the Vice President for Computer & Financial Services and CIO on September 30, 2004.

Social Security Number Usage procedures, policy number 04.75.12, adopted by the Vice President for Computer & Financial Services and CIO on September 30, 2004.

Classification and Handling of Protected Data Policy adopted by the Chief Information Security Officer on January 30, 2014.

University Encryption Guidelines adopted by the Chief Information Security Officer on April 26, 2012.

Guidelines for Storing and Using Personally Identifiable Information in Non-production Environments adopted by the Chief Information Security Officer on April 26, 2012.

Personally Identifiable Information Guidelines adopted by the Chief Information Security Officer on January 12, 2013.

Laptop Security Guidelines adopted by the Chief Information Security Officer on November 14, 2007 reviewed on July 28, 2016.

## 4. Cross References

*Temple Data Rules.* https://its.temple.edu/temple-data-rules

Technology and Software Usage, policy number 04.71.11, at http://policies.temple.edu/

*Information Technology Services Data Classifications*. http://its.temple.edu/data-classifications