Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology and Data Governance Team**
Title:	**Data Governance**
Number:	**ITP-BW-26**
Publish date:	**June 1, 2022**

1.0 Overview

Baldwin Wallace University is hereinafter referred to as "BW". BW authorized user is hereinafter referred to as “user”.

Institutional data are assets maintained to support BW’s central mission of education. To support effective and innovative management, institutional data must be accessible, must correctly represent the information intended, and must be easily integrated across BW’s information technology systems to support the organization’s strategic plans, as well as meet federal and state guidelines and regulations.

BW leadership recognizes the value-added benefits of being able to aggregate information across multiple complex systems and business processes that enable BW to be recognized as a comprehensive university. The Data Governance Team (DGT), in collaboration with the IT Security Governance Team, is responsible for establishing data governance policies, procedures, standards, and guidelines for ensuring the maximum value that BW’s data can be achieved as well as its confidentiality, availability, and integrity.

2.0 Purpose

The purpose of data governance is to develop institution-wide policies and procedures that ensure BW data meets the objectives within and across BW’s administrative and academic data systems. This policy addresses data governance structure and includes sections on data usage, data integration, and data integrity. Directives on data access, data security, data classification, and related topics contained in other IT policies. Adherence to this Data Governance policy and supporting IT policies shall;

- Establish appropriate responsibility for the management of institutional data as an institutional asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Establish publicly available standard definitions for key institutional data to promote data integrity and consistency.
- Improve the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making.

3.0 Scope

“Institutional Data” refers to data elements that are aggregated into metrics relevant to operations, planning, or management of BW in its entirety as applicable, that is reported to BW’s Board of Trustees, federal, state, and any other outside organizations, generally referenced or required for use by more than one organizational unit or included in official administrative reporting.

This policy applies to anyone engaged with BW by employment or contract that creates, manages, or reports these data referenced in the scope above on behalf of BW, or relies on these data for decision making and planning.

Out of scope is data managed and handled only within a single department.

4.0 Policies

4.1 Data Usage

The data governance policy ensures that institutional data are not misused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. The use and access of data depend on the security levels assigned by the Data Owner and on how specific data is classified. Refer to ITP-BW-04 Data Classification Policy, ITS-BW-04-01 Data Classification Standard, and ITG-BW-04-01 Information Protection Guideline for additional information.

BW personnel must access and use data only as required for the performance of their job functions, neither for personal gain nor other inappropriate purposes. See ITP-BW-01 Acceptable Use for more information. They must also access and use data according to the security levels assigned to the data.

Data usage falls into the categories of update and dissemination.

4.1.1 Updating of Data

It is BW policy to follow the principle of least privilege, where users will be provided the least amount of access required to perform their role at BW. This is particularly important as it relates to access to confidential student data. Any user account with access to this type of data must be given the minimum amount of access possible to perform their role. (See ITP-BW-09 Network Access and Authentication Policy.)

Authority to update data that is reported as key institutional data shall be granted solely by the appropriate Data Owner and only to personnel whose job duties specify and require responsibility for data update. Data Owners shall ensure that adequate internal controls and/or change management procedures are in place to manage ‘updates’ to key institutional data, their definitions, and processes.

4.1.2 Dissemination of Data

Dissemination of data must be controlled by following the security practices set forth by the Data Owners via a formal data request process. Appropriate use must be considered before sensitive data are distributed. Only those data elements designated as “directory information” (as defined by ITP-BW-04 Data Classification Policy) can be externally disseminated for official or non-official reporting. The release of directory information should be guided by the need to respect individual privacy and to protect the integrity of the data. The release of all data must be approved following the ITS-BW-04-02 Data Dissemination Standard. The unauthorized dissemination of data to either internal/external personnel is a violation of this policy. Approval by the Data Owner is specific to each request. Data granted for one request is not universally granted for future requests and should not be used for anything other than the original intent. Each new use case must be approved by the Data Owner in a new request or an amendment to the original request regardless of data availability.

4.2 Data Integration

Data integration refers to the ability of data to be assimilated across information systems. It is contingent upon the integrity of the data and the development of a data model, corresponding data structures, and domains. Data model designs should focus on utilizing industry accepted Master Data Management (MDM) methodologies to streamline how data is integrated when applicable.

Downloading individually identifiable data from central systems to electronic files to upload or connect the data to non-central systems (e.g., shadow systems, external vendors) without the knowledge of the Data Owner is prohibited. This practice is not supported and introduces risks associated with data integrity, security, and long-term sustainability of information systems that may not be mitigated due to the nature of the practice.

Documented agreements regarding data use, retention, and responsibility exist with the Data Owners (and vendors in the case of data integration with external entities) of the systems providing and utilizing data.

4.3 Data Integrity

Data systems and/or processes that are involved in the creation of institutional reports must incorporate data integrity and validation rules that ensure the highest levels of data integrity are achieved. Validation rules within data systems may need to include reconciliation routines (checksums, hash totals, record counts) to ensure that software performance meets expected outcomes. Data verification programs such as consistency and reasonableness checks shall be implemented to identify data tampering, errors, and omissions.

4.4 Data Dictionary

A key element of good institutional data governance is to have a common understanding of the meaning of each data element so it, and any derived information, correctly represents the expected information. To meet that requirement, ITS-BW-26-01 Data Dictionary Standard has been established to support this policy. The Data Governance Team is responsible to maintain and update this standard to ensure it is reasonably current.

4.5 Data Mapping

Understanding where the “source of truth” for all institutional data resides is a critical element of any data governance program. The Data Governance Team in partnership with the Information Technology team is responsible to create and maintain that information in ITS-BW-26-02 Data Mapping Standard.

4.6 Responsibilities

The function of applying policies, standards, guidelines, and tools to manage the institution's information resources is termed data governance. 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 will be implemented and maintained.

4.6.1 Executive Sponsor's Responsibilities

Executive Sponsors are cabinet members of BW who are responsible for setting the overall prioritization for institutional business process redesign projects; communicating process transformation priorities across the institution; ensuring project resources are available and adequate to meet established timelines; bringing clarity whenever necessary to project, process and data work; approving data governance policy; appointing members of the DGT. Executive Sponsors will review and make approval decisions on policies presented by the DGT quarterly.

The Executive Sponsors are responsible for the DGT membership. Changes to the DGT membership must be nominated to the DGT. Upon approval, the Executive Sponsors will review and provide an approval decision based on the recommendation. Members are required to attend meetings regularly and review meeting minutes when not in attendance.

4.6.2 Data Governance Team Responsibilities

The Data Governance Team is the body responsible for developing and submitting to Executive Sponsors for approval the data governance policy on data access, data usage, data integrity, and data integration, proposing prioritization of business intelligence work; ensuring that work plans are established and met; and, reporting up to the Executive Sponsors on project status and seeking input on projects that have broad institutional implications related to business intelligence and data. Assignment of personnel to the

key roles listed below requires consensus within the DGT. The group is a self-sustaining committee appointed by the Executive Sponsors.

The DGT is responsible for establishing, developing, modifying, and communicating data standardization and standard reporting practices. A central repository will be maintained and should be referenced for specific guidelines and decision outcomes related to data governance as set forth within this policy.

Documentation (metadata) on institutional data will be maintained within an institutional repository according to specifications provided by the DGT. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic or fiscal calendar.

4.6.3 Data Owner Responsibilities

Data Owners are appointed by functional area senior leadership to develop data-centric policies and carry out the overall administrative data security policies. They have an intricate understanding of the data in their span of control, establish reporting procedures, and recommend changes to data entry practices. Data Owners are responsible for making known the rules and procedures to safeguard the data from unauthorized access and abuse. They are responsible for assuring that census, backup, and retention plans are implemented according to defined needs. They authorize the use of data within their functional area and monitor to verify appropriate data access. They assist institutional data users by providing appropriate documentation and training to support institutional data needs.

It is the responsibility of each Data Owner, in conjunction with the DGT, to determine which core data elements are part of our institutional data.

4.6.4 Data Coordinator's Responsibilities

Data Coordinators manage the data in business processes that result in the data adhering to BW standards. Once data have entered the system, there is a process by which they are validated, transmitted, stored, and archived. The capture and checking are typically based on a functional process or business process. This Data Coordinator role oversees adherence to the business process and in some cases develops the process. While there may be several Data Coordinators, the Data Owners will appoint one as primary for each application. Data Coordinators are also responsible for allowing access to the rules and standards set by the Data Owner for their area. The Data Coordinators should work with the Data Owners for each area to document the agreed-upon procedures that will be followed to administer security access. It is the responsibility of the Data Coordinator to routinely monitor access and ensure that access levels are up to date.

4.7 Applicability of Other Policies

This document is part of BW's cohesive set of policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary. Specifically, directives on data access, data security, data classification, and related topics can be found in other existing IT policies.

5.0 Enforcement

5.1 Employee Enforcement

This policy will be enforced by the Chief Information Security Officer, Chief Information Officer, and BW Administration. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities

or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.

5.2 Student Enforcement

Suspected misuse of the facilities should be reported to the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). The CISO and/or CIO, who is authorized to determine if there has been a violation of policy or law and refer student violators to the Office of Student Conduct for resolution. Pending the outcome, access to the shared technology resources may immediately be restricted or suspended. In some cases, limited access will be provided to the facilities needed for University-related activities, such as classes. Violations can result anywhere from Conduct Probation to suspension or expulsion from the University. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.