Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Data Retention**
Number:	**ITP-BW-06**
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”.

The need to retain data varies widely with the type of data. Some data can be immediately deleted while some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that BW's practices on retention are consistently applied throughout the organization and meet any applicable regulatory requirements.

2.0 Purpose

Data is a valuable commodity, but when retained excessively it can become a financial and/or legal liability. Without a clear retention policy, the volume of data steadily grows, placing an unnecessary cost burden on IT resources. The purpose of this policy is to specify BW's policy for defining and retaining different types of data.

3.0 Scope

The scope of this policy covers all BW owned or processed data stored on BW-owned, BW-leased, or otherwise BW-provided systems and media, regardless of location. Physical copies of this data (printouts, faxes, copies) are also included in the scope.

4.0 Policies

4.1 Reasons for Data Retention

BW does not support a "save everything" approach. That is not practical or cost-effective and would place an excessive cost burden on IT to manage the constantly growing amount of data.

Some data, however, must be retained to protect BW's interests, preserve evidence, and generally conform to responsible business practices. In addition, BW must retain certain information mandated by local, state, federal regulations, accreditation, and other applicable business or regulatory requirements.

4.2 Record Retention

Due to the diversity of data, its uses, and the many regulatory requirements that may affect data, each department that owns a type of data is responsible for developing and publishing a records retention standard that fits the University’s business requirements as well as meets all regulatory requirements.

4.3 Responsibility

The head of each BW department is responsible for:

- Develop the appropriate records retention standards for the data it owns and have it approved by the Data Governance Team.
- Communicate that standard to the rest of the University.
- Train their department members on how to properly comply with all University data retention requirements that are relevant to their positions.
- Create and follow a process that, quarterly, seeks out and securely deletes any data that exceeds retention requirements defined. This process can be either automated or performed manually.
- Inform and coordinate with IT on the automation of appropriate retention policies and ensure all deletion processes are working properly.
- Review their department's retention standards annually to ensure it continues to meet all business and regulatory requirements.

4.4 Data Destruction

Data destruction is a critical component of a data retention policy. Efficient data destruction ensures that BW will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be.

When the retention timeframe expires, BW must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term implications, exceptions must be approved by applicable members of BW's Leadership team.

BW specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or BW policy or under a court-ordered legal hold. Further, any data that may be subject to a subpoena or discovery request must not be destroyed without approval by legal counsel.

4.5 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.

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.