Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Data Backup**
Number:	**ITP-BW-08**
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”.

A backup policy is similar to an insurance policy for operations resilience - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document.

2.0 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup methodology and process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

3.0 Scope

This policy applies to all data stored on BW IT managed systems, Third-Party systems such as cloud services, or local devices.

Excluded from this policy is any data stored on student-owned devices that students may use or come into contact with during their normal educational experience at BW.

4.0 Policies

4.1 Third-Party Systems and Services

Appropriate requirements for proper backup, as specified in this policy, must be included in the contracts with all Third-Parties that process or store BW data. See ITP-BW-16 Outsourcing Policy for more details.

4.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such as backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be important to BW operations and/or employee job functions.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
- Logs and configuration information from network devices such as switches, routers, IDS/IPS systems, etc.

WARNING: It is the user's responsibility to ensure any data of operational importance or long term value is moved to centrally provided storage solutions such as file servers, One Drive, SharePoint,…. as local PC hard drives, personal mobile devices, USB drives, and other end-user devices are **not** backed up.

Example: Your BW provided PC is not backed up. If your hard drive is damaged or fails for any reason, all information on that device may be lost. In some cases, a forensic service may be able to restore some of the data, but the cost will be at the user's expense, not BW as the data should have been placed on a network storage device.

4.2 Not Acceptable Data Backup Methods

The following are not considered acceptable methods of backup and should not be utilized:

- Local PC hard drive, personal mobile devices, USB drives, external portable hard drives.

4.3 Backup Frequency

Backup frequency is critical to successful data recovery. BW has determined that the following minimum backup schedule will allow for sufficient data recovery in the event of an incident while avoiding an undue burden on the users, network, and backup administrator.

Full:	Once per day

4.4 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential data, precautions must be taken that are commensurate to the type of data being stored. BW has set the following requirements for backup storage.

When stored onsite, backup media must be stored in a fireproof container in an access-controlled area. When shipped offsite, a hardened facility (i.e., commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. If a backup service is used, rigorous security procedures must be developed and maintained, which will include, at minimum, credential verification, and the signature of the backup service courier.

Online backups are allowable if the service meets the criteria specified herein. Confidential data must be encrypted using industry-standard, strong encryption to protect BW against data loss.

Note that any third parties involved in the backup process or backup storage must be subjected to the due diligence process as specified in ITP-BW-16 Outsourcing Policy. The security of backup locations, particularly when a third party is involved, must be reviewed at least annually.

4.5 Backup Retention

When determining the time required for backup retention, BW must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving the required data. BW has determined that the following will meet all requirements (note that the backup retention must conform to ITP-BW-06 Retention Policy and any applicable industry requirements):

BW Managed Servers - Full Weekly Backups:	Retained for 18 Weeks
Office 365 – Daily Backups:	30 Days

4.6 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation must include exactly the role of who is responsible for the restoration, how it is performed, under what circumstances it is to be performed, and how long the process should take from request to restoration. The procedures must be clear and concise such that they are not misinterpreted by readers other than the backup administrator or confusing during a time of crisis.

4.7 Restoration Testing

Since a backup policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as once annually.

4.8 Expiration of Backup Media

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service, the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media or a master list. The media must then be retired from service after its time in use exceeds manufacturer specifications.

4.9 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.