Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Data Encryption**
Number:	**ITP-BW-15**
Publish date:	**September 1, 2024**

1.0 Overview

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

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data BW must digitally store increases, the use of encryption must be defined and consistently implemented to ensure the security potential of this technology is realized.

2.0 Purpose

Encryption plays a versatile role in BW’s data security, and many policies contain requirements for encryption. The purpose of this policy is to outline BW's directives for the use of encryption technology so that it is used securely and managed appropriately.

3.0 Scope

This policy covers all data, owned or processed by BW, regardless of whether it is on BW IT resources or BW contracted Third-Party IT resources. For Third-Party solutions, these requirements must be included in the contracts. See ITP-BW-16 Outsourcing Policy for more details.

4.0 Policies

4.1 Data Transmission

Wherever technically possible and financially reasonable, BW requires all data, regardless of its classification, to be transmitted over the internal network to be encrypted using industry-standard strong encryption algorithms to protect BW against data loss.

For data transmissions over private networks or via the Internet, all data, regardless of its classification, should be encrypted using industry-standard strong encryption algorithms to protect BW against data loss.

4.2 Backups

Wherever technically possible and not cost-prohibitive, BW requires backup data to be stored in encrypted form using industry-standard strong encryption algorithms to protect BW against data loss.

4.3 Confidential Data

BW requires confidential data, as defined in the DGP-BW-04 Data Classification Policy, to be stored in encrypted form using industry-standard strong encryption algorithms to protect BW against data loss. Storage is defined as, but is not limited to: a user system, server, database, laptop, USB drive, or any other device that allows for data storage. Any exception due to cost or technical limitations must be approved by the Chief Information Officer.

4.4 Disk Level Encryption

When disk-level encryption is used, the logical access to the encrypted disk must be managed separately from the operating system access control levels where technically reasonable.

4.5 Encryption Key Management

Key management is critical to the success of the implementation of encryption technology. Encryption Keys are to be treated as Level 3: Restricted data as defined by the DGP-BW-04 Data Classification Policy. The following requirements are to be in place to ensure BW always has access to its data,

- All digital keys used on BW Managed Systems must be managed by BW IT.
- To the extent reasonably possible and cost-effective, Third-Party solution keys must be managed by BW IT. It is the Chief Information Officer's discretion to make this judgment decision.
- The Chief Information Officer is responsible for ensuring all keys are managed securely.

4.6 Acceptable Encryption Algorithms

Only the strongest types of generally accepted, non-proprietary encryption algorithms are allowed, as dictated by industry best practices on encryption. The use of proprietary encryption can only be used if specifically approved by the Chief Information Officer since it has not been subjected to public inspection, and its security cannot be assured.

Acceptable algorithms must be reevaluated as encryption technology changes.

4.7 Legal Use

Some governments have regulations applying to the use and import/export of encryption technology. BW must conform to encryption regulations of the local or applicable government.

BW specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so violates this policy and will face immediate consequences per the Enforcement section of this document.

4.8 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 will 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.