Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Physical Security**
Number:	**ITP-BW-17**
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”.

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations, servers, laptops, or any other type of IT device and transmitted on BW's physical network infrastructure. To secure BW data, thought must be given to the security of BW's physical Information Technology (IT) resources to ensure that they are physically protected using appropriate industry methods.

2.0 Purpose

The purpose of this policy is to specify controls to protect BW's physical information systems and technology by setting requirements.

3.0 Scope

This policy only covers the physical security of BW's Information Technology resources and does not include the protection of non-IT items such as campus buildings, vehicles, or the personal safety of employees, students, or visitors.

4.0 Policies.

4.1 Access Controls

Access controls to the Data Center rooms, network closets, and IT equipment storage areas must restrict entry to only approved persons.

4.2 Alarm System

A security alarm system is an excellent way to minimize the risk of theft or reduce loss in the event of a theft. BW mandates the use of a professionally monitored alarm system in crucial areas such as Data Centers. The system must be monitored 24x7, with BW personnel being notified if an alarm is tripped at any time.

4.3 Encryption Security

Due to the open environment nature of a higher education institution, most of the university is open to students and the general public. As such, it is impractical to restrict physical access to most of BW’s end-user IT resources. Therefore, all BW-provided and managed end-user devices that contain sensitive information such as laptops and desktops must have whole disk encryption enabled to protect BW data in the event the device is lost or stolen. See the ITP-BW-15 Encryption Policy for more details.

4.4 Minimizing Risk of Loss and Theft

To minimize the risk of loss or theft of BW IT property, unused IT devices must be stored securely in restricted access storage locations, and data on them should be handled per the ITP-BW-04 Data Classification Policy.

4.5 Fire Prevention

It is BW's policy to provide a safe campus that minimizes the risk of fire. Due to the electrical components of IT systems, the risk of fire in these areas, particularly the Data Center, is typically higher than in other areas of BW's offices. To reduce the impact of fire damage, all members of IT shall attend fire extinguisher training a minimum of every two years. In addition, any member of IT who routinely enters the building housing the BW campus Data Center must be trained on the fire prevention and extinguishing capabilities in that building at a minimum of every two years.

4.6 Termination

When an employee who has access to restricted IT areas such as the Data Centers is terminated, all physical access mechanisms, such as keys, key codes, access cards, etc. must be disabled or recovered immediately.

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.

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.