Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Mobile Devices**
Number:	**ITP-BW-05**
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”.

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, the business use of mobile devices continues to grow. However, as these devices have become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify BW requirements for the use and security of mobile devices.

3.0 Scope

This policy applies to data as it relates to mobile devices that are capable of processing or storing BW data, including, but not limited to, laptops, notebooks, tablet computers, smartphones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with BW data.

Excluded from this policy are any data that students may use or come into contact with during their normal educational experience at BW.

4.0 Policies

4.1 Physical Security

By nature, a mobile device is more susceptible to lose or theft than a non-mobile system. Users of mobile devices must carefully consider the physical security of their devices and take appropriate protective measures, including the following:

- Laptop locks and cables must be used to secure laptops or other mobile devices in locations where a significant risk of theft exists.
- Mobile devices must be kept out of sight and secured when not in use. Example: USB drives not left on the desk where they can be easily stolen.
- Portable media that contains sensitive information, as defined by ITP-BW-04 Data Classification Policy, must be stored in a locked desk, cabinets, or other secured storage areas.
- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting BW data. The following sections specify BW's requirements for data security as it relates to mobile devices. Note that other policies, such as those governing the use of confidential data, may cover these sections in greater detail.

4.2.1 Laptops or Mobile Computers

BW data must be stored on an encrypted disk partition using a strong encryption standard. Laptops must also require a username and passphrase and/or biometrics for login.

4.2.2 Smartphones/Tablets

Strong encryption must be turned on for the entire device. Access to the device must be restricted by either PIN or biometrics.

4.2.3 Removable Media

This section covers any USB drive, flash drive, memory stick, or other removable data storage media that could be connected to BW systems regardless of who owns the device.

All these devices must have strong encryption enabled before placing BW data on them.

4.2.4 Other Mobile Devices

All these devices must have strong encryption enabled before placing BW data on them.

4.3 Connecting non-BW Laptops to BW Business Networks

Users must not connect their non-BW laptop to the BW Business Network without an up-to-date software firewall and up-to-date antivirus/anti-malware application implemented on the laptop. Additionally, the operating system and application software must have all the latest patches installed.

4.4 General Directives

The following directives also apply to the use of mobile devices:

- Loss, theft, or other security incident related to a BW-provided mobile device, or a non-BW device that contains BW data, must be reported promptly to the Help Desk.
- BW data must not be stored on mobile devices unless explicitly authorized for a defined business need. If confidential data is stored on a mobile device it must be appropriately secured and comply with ITP-BW-04 Data Classification Policy, ITS-BW-04-01 Data Classification Standard, and ITG-BW-04-01 Information Protection Guideline.
- Data stored on mobile devices must be securely disposed of per ITP-BW-19 Media Disposal Policy.

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.