Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Wireless Access**
Number:	**ITP-BW-13**
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”.

Wireless communication often plays an important role in the workplace. In the past, some type of wireless access was the exception; it has now become the norm in most organizations. However, while wireless access can increase the mobility and productivity of users, it can also introduce significant security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the control requirements for wireless access to BW's networks. Wireless access can be provided securely if certain steps are taken to mitigate known risks. This policy outlines the controls BW requires to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, software, firmware, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

4.0 Policies

4.1 Physical Guidelines

The physical security of access points must be considered. However, due to the open nature of higher education buildings, access points may be placed in unsecured locations. Where reasonably possible, access points should be installed such that it cannot be easily accessed physically by people in those locations.

4.2 Configuration and Installation

The following requirements apply to the configuration and installation of wireless networks:

4.2.1 Security Configuration

- Wireless access points must not be connected to BW's Business network without a firewall or other form of access control such as a VLAN separating the two networks.
- Encryption must be used to secure communications on wireless networks. The strongest reasonably available algorithm must be used. Insecure standards, such as WEP, are specifically prohibited.
- Administrative access to wireless access points must be changed from default settings and utilize strong passphrases or two-factor authentication when reasonably possible.

- Logging features may be enabled on BW's access points at IT’s discretion.
- Non-Guest wireless networking must require users to authenticate against a centralized server. These connections must be logged,
- Wireless LAN management software may be used by IT to enforce wireless security policies.

4.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated before deployment and a process to maintain the software and/or firmware at current levels in place.
- Wireless networking must not be deployed in a manner that will circumvent BW's security controls.
- Wireless devices must be installed only by BW's IT department or their approved agents.
- Vendor defaults that represent a security risk must be changed, including, but not limited to, passwords, encryption keys, SNMP strings, etc.

4.3 Personal WiFi routers

The use of personal WiFi routers on any BW network is prohibited. Only IT provided and installed WiFi routers, connected to a separate VLAN per section 4.2.1, are permitted to connect to a BW network.

4.4 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.