Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Guest Access**
Number:	**ITP-BW-12**
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”.

Guest access to BW's network is often necessary for visitors, prospective students, consultants, or vendors who are physically visiting BW's campus and offices. Access can be simply in the form of outbound Internet access, or the guest may require access to specific resources on BW's network. Guest access to BW's network must be reasonably managed.

2.0 Purpose

The goals of this policy are to outline appropriate and inappropriate use of Baldwin Wallace University’s guest wireless internet resources, including the use of browsers, email and instant messaging, file uploads and downloads, and media streaming (voice and video). The use of these services is subject to the following conditions.

3.0 Scope

This network is the property of Baldwin Wallace University and may be accessed only by authorized guests.

Guest wireless internet access at Baldwin Wallace University is controlled through the Department of Information Technology. Each user of the Baldwin Wallace University guest wireless system is required to read this internet policy and agree to an acceptable use agreement before receiving a guest wireless internet access account and password.

4.0 Policies

4.1 Governing Laws & Regulations

All users of the Guest wireless network are to comply with federal, state, and local law. All users of the Guest wireless network are required to comply with all BW policies and guidelines.

4.2 Granting Guest Access

Guest access will be provided to any person who is visiting the campus and needs access to the Internet from the BW network. This includes, but is not limited to prospective students, parents, visitors, consultants, or vendors.

4.2.1 Use Agreement Acceptance

Guests must read and accept the Use Agreement as detailed in the ITS-BW-12-01 Guest Access Standard before being granted access.

4.2.2 Security of Guest Systems

Guests are expected to be responsible for maintaining the security of his or her system and ensuring that it is free of viruses, Trojans, malware, etc. BW reserves the right to inspect the system if a security problem is suspected, but will not inspect each guest's system before accessing the network.

BW may use security controls as necessary to keep the network safe from threats that may be introduced from guest computers. This will include network segmentation, as well as the potential use of other tools, such as Intrusion Detection or Intrusion Prevention Systems, monitoring, proxy servers, anti-malware, or other security controls as deemed necessary by the IT.

4.3 Guest Access Infrastructure Requirements

The guest network shall be kept separate from BW the business network and only have access to the Internet. Guess network access to non-internet-facing internal BW systems is not permitted except for certain conference room projection systems as installed by BW IT.

4.4 Monitoring of Guest Access

BW reserves the right to monitor guest access usage to ensure that BW's interests are protected.

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.