Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Remote Access**
Number:	**ITP-BW-03**
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”.

It is often necessary to provide access to BW information resources to employees working outside BW's Business Network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is to define acceptable methods to access BW information technology resources on the Business Network from outside the network. This includes access for any reason from the user's home, remote working locations, while traveling, etc. The purpose is to ensure BW IT resources are protected when used remotely.

3.0 Scope

The scope of this policy covers all employees, contractors, students, and student interns working for BW and external parties that access BW resources over a third-party network, whether such access is performed with BW-provided or non-BW-provided equipment.

4.0 Policies

4.1 Remote Access Methods

All remote access to the BW Business Network must be performed via the BW-provided virtual desktop services. BW will make available the appropriate software to make this connection and passphrase protect access. At the discretion of the Chief Information Officer, BW may further secure remote access with multi-factor authentication techniques.

4.2 Prohibited Actions

Remote access to BW Business Network systems is only to be performed through a BW-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Remote access at the network level, such as a Virtual Private Network (VPN) connection, without written approval from the Chief Information Officer.
- Installing a modem, router, or any other type of remote access device on a BW system or network without the approval of the Chief Information Officer.
- Remotely accessing BW systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC… without written approval from the Chief Information Officer.

- Use of non-BW-provided remote access software.
- Copying data to, and storing data on, remote computers unless explicitly authorized to do so for a defined business need and done in a manner that meets requirements for data confidentiality.

4.3 Use of non-BW-provided Systems

Accessing the BW Business Network resources through a home or public system/network presents a security risk as BW cannot completely control the security of the system/network accessing the BW Business Network. Non-BW-provided computers are allowed to remotely access the BW Business Network, but the users are responsible for following all the appropriate and relevant BW IT policies to ensure their security and the security of BW.

All BW-related work that involves data classified as Level I, or higher, per ITP-BW-04 Data Classification Policy and ITS-BW-04-01 Data Classification Standard must be performed on the BW-provided virtual desktop infrastructure. This includes accessing such data on cloud services in addition to BW-hosted services. No such data is permitted to be processed or stored on non-BW-provided systems.

For remote email access using non-BW-provided mobile devices, see ITP-BW-07 Email Policy.

4.4 Internet Bandwidth for remote access

The remote user is responsible for providing an adequate internet network connection to perform their tasks. BW IT will typically not engage in troubleshooting remote connection issues. The remote user will be directed to work with their internet service provider.

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.