Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**External Connections**
Number:	**ITP-BW-11**
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”.

When the need for a network connection with an external site arises, either a remote office of BW or a third party, the connection must be implemented securely. This can be done in multiple different ways such as site-to-site VPN, a direct WAN connection via a telecom/datacom link,… All types of connections are covered by this policy.

2.0 Purpose

This policy details BW's requirements for site-to-site connections to external sources. The purpose of this policy is to specify the security control requirements for such access to ensure the confidentiality and integrity of the data transmitted and received and to secure the pathways into the network.

3.0 Scope

The scope of this policy covers all permanent (a.k.a. site-to-site) connections to networks external to BW’s owned and managed networks and covers any type of network connection. Note that temporary user remote access such as SSL VPNs are covered under the ITP-BW-03 Remote Access Policy.

4.0 Policies

4.1 Encryption

All site-to-site network connections must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed the current minimum industry best practices.

4.2 Authentication

Site-to-site network connection must utilize a strong authentication, pre-shared key, certificate, or other means of authentication to verify the identity of the remote entity. The strongest, reasonably implemented, authentication method available must be used, which can vary from product to product.

4.3 Implementation

When site-to-site network connections are implemented, they must adhere to the principle of least access, providing access limited to only what is required for business purposes. This separation must be enforced with a firewall or other access control methods that can limit access only to the ports and IP addresses required for business purposes. Further, systems that will be accessed over the site-to-site connection should be located in a demilitarized zone (DMZ), if reasonably possible, to segment access from BW's trusted network.

4.4 Management

BW must manage its network connection gateways, meaning that a third party must not provide and manage both sides of the site-to-site network connection, unless this arrangement is covered under an outsourcing agreement. See ITP-BW-16 Outsourcing Policy for more details. If an existing network connection is to be changed, the changes must only be performed with the approval of the Chief Information Officer.

4.5 Logging and Monitoring

Depending on the nature of the site-to-site network connection, the Chief Information Officer will use his or her discretion as to whether additional logging and monitoring are warranted. As an example, a site-to-site connection to a third party may require additional scrutiny, depending on the access this connection is provided into the network, but a connection to a branch office of BW would likely not be subject to additional logging or monitoring. Generally speaking, connections to third parties must be monitored more closely than internal connections.

4.6 Managing Risk

If a site-to-site network connection is deemed to be a serious security risk, the Chief Information Officer will have the authority to prohibit the connection. If the connection is required for business functions, additional security measures must be taken at the discretion of the Chief Information Officer.

4.7 Restricting Third Party Access

Best practices for connection to a third party require that the link be held to higher security standards than an intra-BW connection. As such, the third party must agree to:

- Restrict access to BW's network to only those users that have a legitimate business need for access.
- Restrict access of those users to only the data and systems they have a business need to access.
- Provide BW with the names and any other relevant information about individuals who will have access to BW data and systems through the connection. BW reserves the right to approve or deny this access based on its risk assessment of the connection.
- Supply BW with on-hours and off-hours contact information for the person or persons responsible for the connection.

Further relevant guidance can be found in the ITP-BW-16 Outsourcing Policy.

4.8 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.