Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Patch and Vulnerability Management**
Number:	**ITP-BW-22**
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”.

This document details the vulnerability management controls required to maintain high levels of system and application security in a diverse IT environment. It outlines the requirements for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain reasonable levels of security.

2.0 Purpose

The purpose of this policy is to ensure that known vulnerabilities in BW IT resources are managed to an acceptable level of risk in a consistent and systematic process.

3.0 Scope

This policy applies to all information processing/computer systems owned by or managed by BW, those entrusted by BW to Third-Parties, and Cloud Services. For non-BW-managed systems, the requirements in this document must be addressed with vendors in contracted service agreements. See ITP-BW-16 Outsourcing Policy for more details.

4.0 Policy

4.1 The Process

Timely information about vulnerabilities in IT resources used by BW shall be gathered, evaluated, and mitigated per the process and timelines defined in ITS-BW-22-01 Patch and Vulnerability Management Standard. The vulnerability management process for all IT resources must be regularly monitored and evaluated to ensure an acceptable level of risk.

4.2 Reporting

Specific information on all risks that are either accepted or not fully mitigated must be documented and reported by the Chief Information Officer to the President’s cabinet and the Risk Management Sub-Committee of the Board of Trustees.

4.3 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 will 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.