Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Penetration Testing**
Number:	**ITP-BW-20**
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”.

The University has an obligation to make sure all services provided are reasonably secured against known attacks. Performance of routine penetration testing is considered an industry best practice to aid in the identification of vulnerabilities that need to be remediated.

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. E.g. It is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings. While each pen test will vary on how they are conducted based on business requirements, several standard frameworks and methodologies exist to guide the conducting of penetration tests. These include the Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), the NIST Special Publication 800-115, the Information System Security Assessment Framework (ISSAF), and the OWASP Testing Guide.

2.0 Purpose

The purpose of this policy is to define the responsibility, and minimum frequency penetration testing must occur.

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

The Chief Information Officer (CIO) and/or Chief Information Security Officer (CISO) are responsible for ensuring:

- Penetration testing is performed against BW-managed IT resources no less than annually. For non-managed IT resources, the CIO/CISO shall ensure the appropriate requirements are contained in the Third-Party contracts.
- All issues identified as a result of the penetration testing are appropriately remediated.

- The penetration testing and remediation are appropriately documented and risks are communicated to BW leadership.

4.2 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.