Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Risk Assessment Framework**
Number:	**ITP-BW-23**
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”.

Organizations must periodically assess the associated IT risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information. This is done to ensure an organization is not operating with either unknown or an unacceptably high level of risk.

2.0 Purpose

The purpose of this policy is to clearly define how BW will assess itself, the frequency of those IT risk assessments, and who is responsible.

3.0 Scope

This policy applies to all information processing/computer systems owned and managed by BW IT, those entrusted by BW to Third-Parties and Cloud Services, as well as end-users of those systems and any BW data they have transferred into their possession either electronically or on paper. 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.

Out of scope are students and their respective devices, as well as BW, purchased informatics devices unauthorized by or outside of the IT span of control.

4.0 Policy

4.1 Assessments and Frameworks

Baldwin Wallace University, being a higher education facility that is involved in every aspect of student living and education, houses a medical facility, payment centers, financial/loan services, and capture of student information. As such, BW is subject to many cybersecurity standards with the following applicable cybersecurity standards having been identified as a priority:

- HIPAA (Med Center and Athletic Medicine)
- PCI-DSS (Point of sale, bursar’s office)
- FERPA (Colleague, Enrollment, online directories, trusted partners)
- FTC’s Red Flag Rules
- SOC 2, GLBA (Giving programs, Financial Aid)
- State of Ohio Laws: Title XXXIII ORC 3319.321(B)

BW has standardized on the NIST Cyber Security Framework (CSF) as its overarching set of IT Security controls and will assess itself against NIST CSF in addition to the above-mandated control frameworks where applicable.

The Chief Information Security Officer (CISO) is responsible for conducting a security assessment (or contracting it to be conducted) every two years. The risk assessment will be based on NIST CSF, and the results reported to the Chief Information Officer (CIO). The CIO will, in turn, report the results to the President's cabinet and the Risk Management Sub-Committee of the Board of Trustees with the appropriate recommendations on how to effectively mitigate any significant deficiencies that were identified.

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 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.