Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Security Awareness**
Number:	**ITP-BW-21**
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”.

Security breaches have grave consequences for organizations. The average cost of university data breaches continues to rise each year, and for some universities, breaches can additionally lead to undesired downtimes. At the same time, attack methods against end-user via e-mail, voice, and social media have grown and become increasingly sophisticated, making them more effective. The Verizon DBIR has shown that end-users are typical at the start of a successful breach 80-90% of the time. Thus, it is imperative that end-user security awareness training is implemented to prevent such attacks as it can reduce the costs of running a business by reducing the number of cyber incidents.

2.0 Purpose

The purpose of this policy is to communicate the requirements of information security awareness training and to inform and highlight the responsibilities faculty, staff, and certain student workers, third-party contractors, and volunteers have regarding their information security obligations. Formal training will aid in the protection of data, personal, intellectual property, financial, or restricted and sensitive information, networked systems, and applications entrusted to and utilized by the University, by providing a broad understanding of information security threats, risks, and best practices.

3.0 Scope

Faculty, Staff, Student Workers, and other individuals with access to sensitive data:

This policy applies to all faculty, staff, student workers, and other individuals with access to sensitive data. As members of the BW community, each individual is accountable and must demonstrate an understanding of their unique role and responsibility as the best defense to ensure the protection of the University’s information, data, and reputation.

Third-Party Contractors (defined as vendors, consultants – non-BW employees):

Third-Party contractors who have access to BW data or systems in the course of their employment or volunteer activities are also covered by this policy. When working for or providing services on behalf of BW, Third-Party contractors are accountable and must demonstrate an equivalent understanding and training for their role and responsibility to ensure the protection of the University’s information, data, and reputation.

4.0 Policy

Information Technology is responsible for the information security awareness program, training, education, and awareness communication for the University. The program will include an enhanced understanding and appreciation of information risks, services that Information Technology provides, information about the threats, techniques, and consequences to the University; information on reporting incidents; guidance, and resources to protect information and devices at work and remotely.

4.1 Faculty, Staff, Student Workers, and other individuals with access to sensitive data:

Formal participation and review of the security awareness program are mandatory for all full-time and part-time faculty, staff, and other individuals with access to sensitive data every year. Newly hired faculty and staff are required to complete the training within thirty days of their hire date. The requirement for a review every year shall be superseded by an incident or information indicating a need for immediate intervention and training by a specific department, or the entire University. Additional topic-specific training may be required, based on role, information type access/use (e.g., PCI-DSS, FERPA, Research, HIPAA, etc.), or identified increased risk. Student workers and other individuals with access to sensitive data are also required to complete training within thirty days of their start date. It is the responsibility of the individual's supervisor to ensure that these persons complete this requirement.

BW Information Technology will coordinate, monitor, and track the completion of the required Security Awareness program. University Vice Presidents and Deans are required to ensure adherence to the policy, and completion of the required program. Program content will be updated yearly to reflect current security trends, threats, techniques, and the evolving environment of information security.

Failure to comply with this policy may result in denial or removal of access privileges to BW's electronic systems (such as e-mail and the BW network).

4.2 Third-Party Contractors:

Formal participation and review of a security awareness program for Third-Party Contractors who have access to BW Data or systems in the course of their academic, employment, or service activities is mandatory as a condition of Third-Party Contractor engagement. Third-Party contractors are accountable and must demonstrate an equivalent understanding and training for their role and responsibility to ensure the protection of the University's information, data, and reputation.

Failure to comply with this policy may result in denial or removal of access privileges to BW's electronic systems (such as e-mail and the BW network).

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.