Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Passphrases**
Number:	**ITP-BW-02**
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”.

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

Past techniques of password construction are no longer effective. As such, BW will be using a passphrase model for password construction.

2.0 Purpose

The purpose of this policy is to specify how to construct and use passphrases. Most importantly, this policy will help users understand why strong passphrases are a necessity and help them create passphrases that are both secure and useable. Lastly, this policy will educate users on the secure use of passphrases.

3.0 Scope

This policy applies to every IT account provided on any network, system, device, or service provided by BW.

4.0 Policies

4.1 Construction

The best security against a password incident is to follow a sound passphrase construction strategy. The organization mandates that users must use as many words or characters as reasonably possible concerning the capabilities of the system they are constructing a passphrase for. See ITS-BW-02-01 Passphrase Standard for details.

4.2 Confidentiality

Login credentials (passphrases and passwords) are considered confidential data and treated with the same discretion as any of the organization's confidential information.

4.3 Change Frequency

To maintain good security, passphrases may be required to periodically change based on length. This limits the damage an attacker can do as well as helps to frustrate and slow attempts to crack a passphrase through brute force. See the Passphrase Standard for change frequency details. The university may use software that enforces this policy by expiring users' passphrases periodically.

4.4 Passphrase reuse

Due to the many attacks on public websites and their loss of User IDs and passwords/passphrases, users are required to make BW passphrases unique from any other passwords or passphrases they use for personal use. In addition, when selecting a new passphrase, users must not select a passphrase that is substantially the same as, or similar to, any of the previous passphrases used.

4.5 Incident Reporting

Since the compromise of a single passphrase can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passphrases to the BW HelpDesk and immediately change the passphrase in question. Any request for passphrases over the phone or email, whether the request came from organization personnel or not, must be expediently reported. When a passphrase is suspected to have been compromised BW IT will request that the user, or users, change all his or her passphrases.

4.5 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.