Baldwin Wallace University Information Technology Standard

Issued by:	**Information Technology**
Title:	**Passphrase Standard**
Number:	**ITS-BW-02-01**
Publish date:	**September 1, 2024**

A. Passphrase Generation

This document defines the required components of the passphrase construction process to mitigate the risks associated with poorly constructed login credentials. This process consists of three steps, as shown below:

NOTE: The longer the password, the stronger it is!

Step 1. Identify the system's limits:

The goal of this step is to identify the limits associated with a system's credential system. Different systems will have different limits on the number of characters a passphrase is allowed to contain, and what characteristics the passphrase must contain. The following table contains example credential limits and their vulnerabilities. This table is not exhaustive but should provide a good framework for understanding how the differences in system capabilities affect the security of passphrases.

Limit	Vulnerability to Cracking Techniques
1-8 Character Limit	Passphrases can be cracked in a much shorter time than those of greater length. The passphrase most likely will not contain more than two words.
9-16 Character Limit	The passphrase is harder to crack, and can easily contain more than two words.
17-32 Character Limit	The passphrase is significantly more difficult to crack, and can easily contain more than four words.
33-64 Character Limit	The passphrase is impossible to crack, and can easily contain more than six words.

Step 2. Construct a Passphrase:

System limits identified in Step 1 must be factored into passphrase generation. Passphrases should be made of words strung together into a phrase, which can be modified to fit within a system's requirements.

Limit	Best Practices for Passphrase Construction
1-8 Character Limit	String together two words. Example passphrases: No special character or number requirements: "BlueTire" Numbers and special characters required:

🟥	“BluT1re!”
9-16 Character Limit	String together more than two words. Example passphrases: No special character or number requirements: “SunWalkRainDrive” Numbers and special characters required: “SunWalkRa!nDriv3”
17-32 Character Limit	String together more than four words. NOTE: Spaces are acceptable to use. Example passphrases: No special character or number requirements: “Isn't Minnesota Colder Than Wisconsin.” Numbers and special characters required: “Is Minnesota 9 Colder Than Wisconsin?”
33-64 Character Limit	String together more than six words. NOTE: Spaces are acceptable to use. Example passphrases: No special character or number requirements: “Correctly Formed Credentials With Multiple Complex Interconnected Words” Numbers and special characters required: “4096 Correctly Formed Credentials With Multiple Complex Connected Words!”

B. Passphrase Confidentiality

Passphrases are considered confidential data under the BW Data Classification Policy and treated with the same discretion as any other confidential data. The following rules apply to the confidentiality of university passphrases:

- Users must not disclose their credentials to anyone. *This includes IT personnel.*
- Users must not share their credentials with others (co-workers, supervisors, family, etc.).
- Users must not write down their credentials and leave them unsecured.
- Users must not check the "save password" box when authenticating to applications.
- Users must not use the same passphrase for different systems and/or accounts.
- Users must not send passphrases via email.
- Users must not re-use passphrases.

C. Passphrase Reconstruction

To mitigate passphrase incidents, passphrases must be changed regularly. The time of use for each length of a password is described in four categories below:

C.1 – 8 Character Passphrases (RED)

- Passphrase is vulnerable to cracking attempts at this length.
- Passphrase should be changed bi-annually.

C.2 – 9-16 Character Passphrases (ORANGE)

- Passphrase is less vulnerable to cracking attempts at this length.
- Passphrase should be changed annually

C.3 – 17-32 Character Passphrases (YELLOW)

- Passphrase is more resilient to cracking attempts at this length.
- Passphrase should be changed biennially.

C.3 – 33-64 Character Passphrases (GREEN)

- Passphrase is very resilient to cracking attempts at this length.
- Passphrase does not need to be changed.

D. Summary Matrix

The standards above are presented here in tabular form to aid in understanding.

	Category 1 (1-8 Characters)	Category 2 (9-16 Characters)	Category 3 (17-32 Characters)	Category 4 (33-64 Characters)
Strength	Weak	Medium	Strong	Very Strong
When to change	Bi-Annually	Annually	Biennially	N/A