

# Bates College Passphrase Policy

## 1. Purpose

To establish secure passphrase requirements aligned with best practices and current National Institute of Standards and Technology (NIST) guidelines, ensuring the protection of Bates College's information systems and data.

## 2. Scope

This policy applies to all students, faculty, staff, contractors, vendors, and other authorized users who have access to Bates College information systems, including systems hosted or maintained by third-party service providers that store, process, or access Bates College data.

## 3. Passphrase Requirements:

- Minimum length: 18 characters
  - Bates College requires passphrases to be at least 18 characters long for accounts used to access Bates College systems, services, or data.
  - For legacy or third-party systems that do not support 18-character passwords, the longest allowable password must be used.
  - System owners are expected to work with ILS to identify and phase out systems that cannot support minimum password standards.

Encouraged (Do this)	Avoid (Don't do this)
<b>Unrelated words:</b> Use 4+ random non-sentence words that don't relate to each other (e.g., <b>pencil truck garden window</b> ).	<b>Natural Sentences:</b> Avoid phrases that follow grammar or express a single idea (e.g., <b>I love my green pumpkin</b> ).
<b>Personally meaningful:</b> Use words that are easy for <i>you</i> to visualize but hard for others to guess.	<b>Common Quotes:</b> Do not use song lyrics, passages from books, movie quotes, or other well-known phrases.
<b>Random sequence:</b> Ensure the words don't form a sentence, follow normal grammar, or express a single idea or theme	<b>Predictable Patterns:</b> Avoid keyboard paths (e.g., <b>qawsed12345</b> ) or sequential numbers.
<b>Unique to you:</b> Create something that cannot be found in a dictionary or a list of common phrases online.	<b>Public References:</b> Avoid using "Bates College," your username, or easily discoverable personal info.

- Examples:
  - candle velvet train tab – 23 characters
  - cable boppie collar lamp – 24 characters
  - Measurepurple carbide so – 24 characters
  - teapot glacier orbit violin – 27 characters

Note: While you can use capital letters, numbers, or symbols, they are not required. Focus on randomness and length.

#### 4. Password Expiration and Reset

- Routine password resets (e.g., annual resets) are no longer required unless there is evidence of compromise or suspected compromise.
- System or shared account passwords must be changed when an employee with access to those credentials leaves the College.
- Passwords must be changed immediately if a security incident or unauthorized use is suspected.
- Bates College may periodically perform checks against known compromised credentials to proactively identify vulnerable passwords.
- Some third-party systems or services may enforce fixed password reset intervals due to their own compliance or technical requirements. In these cases, users are expected to follow the system-specific password change prompts while still complying with the overall principles of this policy.

#### 5. Protection and Handling of Passwords

- Passwords must be treated as restricted data.
- Sharing of user credentials for individual user accounts is strictly prohibited.
- Storing of passwords in a web browser is strictly prohibited.
- Users should avoid writing down passwords. If necessary, passwords may be securely stored in a password manager. The only ILS-approved password manager is 1Password. 1Password accounts are provisioned by ILS, and the cost of the license(s) is charged to the requesting department.

#### 6. Account Lockout

- User accounts may lock in some cases after 5 failed login attempts to prevent unauthorized access. Accounts must be unlocked by contacting the IT Help Desk or through an approved automated process.
- Systems may implement progressive delays or throttling after failed login attempts to minimize the risk of denial-of-service scenarios.

## 7. Multi-Factor Authentication (MFA)

MFA is required for all users, as well as for users accessing critical or sensitive Bates College systems or third-party systems that hold Bates data.