Bates College Password Policy

1. Purpose

To establish secure password requirements aligned with best practices and current National Institute of Standards and Technology (NIST) guidelines, ensuring 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. Password Requirements:

- Minimum length: 18 characters
  - Bates College sets a minimum passphrase length of 18 characters for systems it directly manages or integrates with Single Sign-On (SSO). There is no longer a requirement for capitalization, numbers, or special characters.
  - 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.

- Users are encouraged to create a memorable passphrase composed of unrelated and random but personally meaningful words or concepts. Avoid using common phrases, quotes, song lyrics, book lines, keyboard patterns (e.g., qwerty7890, asdfghjkl;), or public references. A strong passphrase should be unique to you and not easily found online or guessed by others.
  - Examples:
    - My favorite smell is french – 27 characters
    - our car runs off dreams – 23 characters
    - houndstoothiscomingback – 23 characters
    - candle velvet train – 19 characters

(These examples show that long, memorable phrases made from unrelated words can be strong passphrases—even without uppercase letters, numbers, or special characters. Just ensure yours is unique and not easily guessed.)

- You can use capital letters, numbers, symbols, or spaces—but you don't have to. Just focus on making it long and unique.

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 passwords 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.