ALMA COLLEGE

Password Policy

Purpose

Usernames and passwords are how information systems establish user identity. Passwords are a key means of managing campus information system and service access. Alma College account holders are responsible for taking appropriate steps, as outlined below, to select and secure their passwords.

Policy

Individuals are responsible for creating secure passwords and keeping them confidential. The following requirements must be adhered when creating and managing passwords.

Personal Account Password Requirements

- Passwords for College accounts must never be reused for non-Alma services
- Passwords must never be shared, even with Information Technology Services (ITS) staff
- Default passwords must be changed immediately upon first use
- Passwords must not be written down and left unsecured. This includes both paper and unprotected digital formats.
- Passwords should not be stored in web browser password managers
- Personal account passwords must:
    - be at least (8) characters in length
    - contain 3 of the 4 following character sets: lower case alpha, upper case alpha, special characters, and numbers
    - be changed at least annually

System Administrator and Service Account Password Requirements

- Administrative and service passwords must
    - be at least (14) characters in length
    - contain 3 of the 4 following character sets: lower case alpha, upper case alpha, special characters, and numbers
- Service account passwords must never be stored unencrypted as part of a script, program, or automated process
- Service accounts, or credentials granting administrative rights must be securely stored in the College's privileged access management system
- Two factor authentication should be used whenever possible with credentials granting privileged access

Violations

Violations may be referred to Human Resources or the office of Student Affairs.