ALMA COLLEGE

Password Policy

Purpose

Usernames and passwords are how information systems establish user identity. Passwords are a key means of managing access to information systems and services and preventing unauthorized use. Alma College account holders are responsible for taking appropriate steps, as outlined below, to select their password and keep it confidential.

Policy

Personal Account Password Requirements

- Alma College account passwords may not be reused with non-Alma services
- Passwords must never be shared
- Default passwords must be changed immediately upon first use
- Passwords may not be written down and left unsecured. This includes both paper and digital formats.
- Passwords may not be stored in web browser password managers
- Personal account passwords must be:
    - at least (14) characters in length
    - changed at least annually

Additional requirements for privileged accounts, system administrators and service account passwords:

- 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 accounts, or credentials granting administrative rights or privileged access must be securely stored in the College's Privileged Access Management system
- Service account passwords must never be stored unencrypted e.g. in scripts, program code, or automated processes
- Two factor authentication must be used whenever possible with credentials granting privileged access

Violations

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

Updated 9/16/2022