Prescott College	**Policy Number:**	
	Policy Category: *Information Technology Policies*	
	Password Policy	
	Policy Summary: *This policy defines standards, procedures, and restrictions for any and all end users' passwords for Prescott College systems.*	
	Approval Date: *03/25/24*	**Effective Date:** *Upon approval*
Policy Owner: Vice President, Finance and Administration	**Scheduled for Review:** *Spring 2029*	

Policy Statement

The following guidelines for effectively creating, maintaining, and protecting passwords at Prescott College must be followed.

Password Creation

1. All user and admin passwords must be at least 8 characters in length and contain characters from three of the following four categories:
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example: !, $, #, %)
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.

Password Aging

User passwords must be changed every 12 months. Previously used passwords may not be reused.

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")

Enforcement

1. The end user is responsible to ensure enforcement with the policies above.

2. Users who believe their password may have been compromised, should **immediately** report the incident to helpdesk@prescott.edu and change the password.
3. Failure to comply with this policy may result in the suspension of any or all technology use and connectivity privileges, disciplinary actions and possibly termination of employment.

Definitions

Reason for Policy

To protect the integrity of the confidential client and business data that resides within Prescott College's technology infrastructure, including internal and external cloud services.

Responsibilities	
For following policy:	All persons using a mobile device to access, store, backup or relocate any enterprise data.
For enforcement of policy:	Director, Information Technology
For oversight of policy:	Director, Information Technology
For procedures implementing the policy:	Director, Information Technology
For notification:	Policy Librarian

Procedures

Cross Referenced Policies

Revision History