CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
OP. 608	**Vice President, Finance and Administration**		
Policy Name			
Password Policy			
Approved by	Replaces	Category	Next Review
SLC	**New**		**February 2026**
Date Issued	Date Revised	Related Policies, Reference	
February 2023		**OP.604 Acceptable Use and Security of Electronic Information and Technology** **E.602 Student Email** **E.603 Employee Email Policy**	

1 PURPOSE

Capilano University is committed to a secure information technology environment for all staff, faculty, students, and third-party contractors.

The purpose of this policy is to establish the standards for the proper construction, usage, handling, and maintenance of all Capilano University's (the University) accounts passwords; and to ensure that all users are aware of their responsibilities in effective password management.

2 DEFINITIONS

"**Authentication"** refers to verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

"**Compromised Account"** refers to an account that is or has been accessed by an unauthorized party, prior to the password being changed by the authorized user.

"Employee" means any person employed by the University.

"**Identity"** refers to the set of physical and behavioral characteristics by which an individual is uniquely recognizable.

***"*Identity verification"** refers to a procedure for verifying users' identities using government-issued photo identifications and dates of birth.

"Information Technology (IT)" refers to computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data.

***"*IT Service Account"** refers to an account used by an information technology resource to contact or interface with another information technology resource.

"**Member of the University Community**" means employees, students, agents, board members and volunteers.

"Multi-Factor Authentication (MFA)" refers to an authentication system that requires more than one distinct authentication factor for successful authentication.

"Multi-Factor Authentication Registered (MFA)" refers to those user accounts that have successfully completed the MFA registration process.

"Password" means a trusted secret used for authentication**.**

"Student" means an individual enrolled in any course (credit or non-credit) at the University

"**Users**" refers to all Members of the University Community, and any other individuals including, alumni, service providers and their subcontractors (e.g., persons or corporate entities retained under a contract to perform services for the University) and visitors (guests) who have access to the University's network, systems, or applications.

3 SCOPE

This policy applies to all Users, including Technical Administrator accounts, who access and authenticate to the University's network, systems, and applications whether on-campus or remotely, and whether in on-premises or cloud environments.

4 POLICY STATEMENT

4.1 All University systems and applications must be structured to comply with the Capilano University Password Standards (the 'Password Standards") within the capabilities of the University systems or applications. IT Services will maintain the Password Standards which will be posted on the IT Services Accounts, Logins & Passwords page. All changes to the Password Standard require approval of the Chief Information Officer.

4.2 Prior to installation or deployment, all default passwords on any information system components, and endpoints, must be changed to unique passwords that match the minimum requirements set out in the Password Standards.

4.3 The University will require third party service providers whose work on behalf of the University involves access to the University's network, systems, and applications to adhere to the Password Standards. Non-compliance will be considered as a breach of their contract with the University.

4.4 Passwords for University accounts are considered confidential information. Under no circumstances should a user share or hint at their password to another individual, including any

University employees. IT department members will never request that Users disclose their account passwords.

4.5 Users must not:

a) say their password aloud in public or in front of others;
b) write or store their password in plain text;
c) share their passwords in email, online chat, electronic forms, or other electronic communications with anyone; and
d) use the "Remember Password" feature of web browsers.

4.6 IT administrators will require passwords are changed in line with the Password Standards or as needed in response to security intelligence information.

4.7 Users will be notified at least fourteen days in advance of their account password expiration. Users must make every attempt to update their account password upon receiving the password expiration notification by using the University's self-service password reset services.

4.8 Users with expired account passwords shall use University self-service password reset services.

4.9 Users who have forgotten their account passwords and are unable to reset them using University self-service password reset services must contact IT services and provide identity verification.

4.10 If a user believes or suspects that their account password has been compromised, they must immediately change their password using the University self-service password reset services or contact the University IT services immediately.

5. DESIGNATED OFFICER

5.1 The Vice President, Finance and Administration is the Policy Owner responsible for the oversight of this Policy. The administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Chief Information Officer.

6. REVIEW AND AMENDMENT

6.1 This Policy and associated procedure will be reviewed on a regular basis and amended as required in accordance with Policy B.102 Policy Development and Management.