| 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** | | **IM&DT** | **February 2026** |
| Date Issued | Date Revised | Related Policies | |
| **February 22, 2023** | **January 24, 2024** | **OP.604 Acceptable Use and Security of Digital Technology**<br>**OP.602 Student Email Policy**<br>**OP.603 Employee Email Policy** | |

## 1 PURPOSE

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

1.2 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.

1.3 The Digital Technology Services Office will develop and maintain Password Standards to support this policy as part of the set of Digital Technology standards, made available on the Digital Technology Services pages of the Frontlines website.

## 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"** refers to access by an unauthorized party.

**"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.

**"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.

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

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

**"Privileged Access"** means having special access to information or systems or abilities to perform functions above that of a normal User. Privileged access is granted on the basis of the individual's role for the sole purpose of completing work related activities.

**"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 and User accounts, including accounts with Privileged Access 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 systems and applications owned and operated by Capilano University must support the Password Standards in the device and User Authentication process.

a) Users will be directed to the Password Standards on the Digital Technology Services Accounts, Logins & Passwords page. Access to this page is provided to all Users authorized to access the University's network, as part of their onboarding process.

b) All changes to the Password Standard require approval of the Associate Vice President, Digital Technology Services

4.2 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.

4.3 If a system that is required to deliver a University program or activity cannot comply with the Password Standards, a variance request must be submitted to the Associate Vice President, Digital Technology Services for review. Exceptions will only be granted on an individual basis to systems that do not collect, use or store personal information or have the potential to grant broader network system access.

4.4 During user account creation, expiration of first-time pre-assigned passwords must be enforced on all user accounts, and all systems and applications of the University shall be configured to support this requirement. At the time of initial login, the user must change to a unique password, which shall meet the minimum requirements set out in the Password Standards.

4.5 Passwords for University accounts are considered confidential information. Under no circumstances shall a User share their password with another individual, including University employees and supervisors. No members of the University, specifically Digital Technology Services shall request that Users disclose their account passwords.

4.6 Users shall not:

a) disclose their password in any manner to others, including via email, online chat, electronic forms, or other electronic communications;

b) write or store their password in plain text or in any easily reversible form;

c) use the password caching feature found in web applications, including web browsers; or

d) reuse the same password across multiple accounts.

4.7 Passwords may be stored in a password manager or secure password storage application that has been duly authorized for use by the University.

4.8 Users shall be notified 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 Users with expired account Passwords shall use University self-service Password reset services.

4.9 Users who do not remember their account Passwords and are unable to reset them using University self-service Password reset services must contact Digital Technology Services and provide verification of their Identity. Expiration of pre-assigned Passwords must be enforced during the manual Password reset procedure.

4.10 If a User suspects or discovers that their account Password may have been Compromised, they must immediately change their Password using the University self-service Password reset services and report the incident to Digital Technology Services.

## 5. DESIGNATED OFFICER

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 Associate Vice President Digital Technology Services.