

 CAPILANO UNIVERSITY		PASSWORD STANDARDS	
Date Issued		Date Revised	
February 2023		NEW	
		Related Policies, Reference	
		OP.608 Password Policy	

1 DEFINITIONS

“Standard User Account” refers to an account with limited or no ability to modify system resources, settings, or programs

“Technical Administrator Accounts” refers to an account with elevated, unrestricted access that any IT administrator or eligible individuals approved by IT may use to execute administrative functions on any information system or application.

“Weak passwords” are passwords that are short, common, a system default, or anything else that can be easily guessed by using a subset of all possible passwords in a password-cracking attempt.

2 PASSWORD CONSTRUCTION

2.1 Passwords used to gain access to the University systems and applications must be unique; and must not be used for non-University services, including but not limited to personal banking, online shopping sites, and social media sites

2.2 Passwords must be:

- a) A minimum of fourteen (14) characters long for standard user accounts; and
- b) A minimum of sixteen (16) characters long for technical administrator accounts.

2.3 Account passwords must not contain:

- a) the user’s given name, surname, or preferred name;
- b) the user’s Capilano University username;
- c) student number or employee number;
- d) previously used password; and
- e) a known compromised or commonly used weak password.

2.4 Passwords must be changed at a minimum every calendar year (365 days), however there is no expiry for service accounts.