


Procedure Name:	IT PASSWORD AND AUTHENTICATION	
Approved By:	President's Council & Board of Governors	
Approval Date:	September 5, 2025	
Next Scheduled Renewal Date:	August 2030	
Procedure Holder:	VP, Corporate Services & CFO	
Operational Lead:	Director, Information Technology/CIO	
Procedure Number:	INF-004P	

IT PASSWORD AND AUTHENTICATION PROCEDURE

1.00 PURPOSE

- 1.1 The purpose is as set out in the policy.

2.00 DEFINITIONS

- 2.1 **Account:** For purposes of this procedure, an account is an electronic identifier used by systems and applications to authenticate and authorize Users or processes to access College technology resources and to facilitate auditing of activities associated with an individual User.
- 2.2 **Account Manager:** An individual or system that manages accounts, assigns accounts to individuals, and grants privileges to accounts.
- 2.3 **Account Type:**
 - a. **Functional:** Account used by applications and processes and not interactively used by end Users.
 - b. **Inactive:** Any account that has not been used to access the organization's systems or services for a specified period of time.
 - c. **Individual:** Primary account assigned to a single individual for access to technology resources, including interactive log-on to computers, email, virtual private networks (VPNs), or other Coast Mountain College (CMTN) resources.
 - d. **Least Privilege:** Accounts in which Users, applications, and systems are granted the minimum level of access—or permissions—necessary to perform their authorized functions. This reduces the risk of accidental or malicious misuse of systems or data. Access rights should be limited in scope and duration, and elevated privileges should be assigned only when explicitly required and appropriately approved.
 - e. **Privileged:** Administrative account restricted to authorized Information Technology (IT) staff.
 - f. **Service:** An account used by services or applications to interact with other systems. These accounts are not tied to specific Users but are used for automation or system processes, such as running background jobs, managing databases, or providing

application interfaces (e.g., web server accounts, database connection accounts, backup systems).

- g. **Shared:** Account used or shared where multiple Users know the password or otherwise use the account for interactive log-on.
- h. **Unprivileged:** An account, typically an individual User account, that does not have administrative or elevated access rights. Unprivileged accounts are used for routine activities (e.g., email, document access) and must follow the principle of least privilege. In some cases, functional or system accounts may also be designated as unprivileged if they operate with restricted permissions and no administrative capabilities.

- 2.4 **Active Student:** A student who is currently enrolled in one or more credit-bearing or continuing education courses in the current academic term, or who has a confirmed registration for a future term. Active students are considered to have a current affiliation with the College and may be eligible for access to College IT systems and services as defined by IT standards.

Note: Not all continuing education students may be granted accounts by default; access will depend on program type and business need.

- 2.5 **API Token:** For the purposes of this procedure, an application program interface (API) token is a unique, long, token or key that may provide authentication for an application to access another service or application.
- 2.6 **Authentication:** The process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized. Authentication factors may include something you know (e.g., password), something you have (e.g., hardware token, certificate, or software authenticator), or something you are (usually a biometric, like a fingerprint).
- 2.7 **Authorization:** A process by which access to a resource is authorized based upon the authenticated identity or account.
- 2.8 **Biometric Identifier:** Unique physical or behavioral characteristics of a person that can be analyzed to uniquely identify and authenticate a person to an account for accessing a technology resource.
- 2.9 **Federated Identity:** An account which can be used across disparate technology systems or organizations, typically through a single sign-on (SSO) service.
- 2.10 **Geolocation:** For purposes of this procedure, geolocation refers to the process of identifying the locations of a User based upon the known locations of their Internet protocol (IP) addresses, or from data collected from their authenticated devices with built-in location detection.
- 2.11 **Inactive Student:** A student who is not enrolled in the current or upcoming academic term and does not have a confirmed future registration. Inactive students may have their access to IT systems restricted or disabled in accordance with account lifecycle management and retention policies.

Note: For the purposes of this procedure, inactive status may also apply to accounts associated with students who remain enrolled but whose accounts have experienced extended periods of inactivity as determined by IT operational standards and policies.

- 2.12 **Information Technology (IT):** For the purpose of this procedure, IT refers to the Information Technology Department.
- 2.13 **Multi-Factor Authentication (MFA):** Using two or more authentication factors: typically, passwords, biometrics, or tokens, to achieve authentication.
- 2.14 **Password:** A combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase.
- 2.15 **Personal Identification Number (PIN):** A short number or password used locally on a device as a convenient authentication alternative to typing a full password.
- 2.16 **Single Sign-On:** Use of a single account to access multiple applications or systems.
- 2.17 **The College:** Coast Mountain College (CMTN).
- 2.18 **Token:** A hardware or software device that can be cryptographically verified as unique.
- 2.19 **User Identifier:** Any unique piece of information that identifies an individual within the system, such as a username, email address, or biometric data. This identifier is used alongside authentication credentials (such as a password or security token) to verify the User's identity.

3.00 PASSWORD AND AUTHENTICATION PROCEDURES

- 3.1 Access to a host computer system, network server, or networked personal computer must be approved by the systems owner, who forwards a request for access to the IT Helpdesk.
- 3.2 A User's manager will approve the User's access to a computer system, network, or servers by sending a request for access to the Information Technology (IT) Helpdesk.
- 3.3 IT will:
 - a. maintain User identifier information and keep system access requests on file
 - b. supply the User with an identifier and a password for first-time access
 - c. publish password complexity standards within their knowledge base.
- 3.4 Where appropriate, Users will be required to use two-factor authentication.
- 3.5 A User:
 - a. may access College systems and networks by providing the required authentication.
 - b. must change a password immediately if they have reason to believe or suspect that it is no longer confidential.

4.00 RESPONSIBILITIES

- 4.1 Authentication of Users and applications that access or process data is a fundamental requirement of information security to ensure the confidentiality and integrity of data.
- 4.2 This procedure establishes authentication requirements for the use of the College's technology resources.

5.00 RESPONSIBILITY OF USERS

- 5.1 Users are responsible for keeping passwords and all other types of authentication secure and confidential, including not sharing or storing passwords in an insecure manner.

6.00 PASSWORDS

- 6.1 Passwords are confidential College information and should never be stored electronically without strong encryption.
- 6.2 All passwords must be changed at first issuance or use.
- 6.3 Passwords should not be written down and/or left in an easily accessible location.
- 6.4 Passwords must not be shared for any individual accounts, including with IT support professionals, and only shared for other account types as defined in Section 2.3 of this procedure to the minimum extent required.
 - a. If anyone asks a User for their password (including IT staff), they are obligated to report this to IT through the Service Desk (<https://cmtn.teamdynamix.com/>) as a security incident.
- 6.5 For any shared passwords, whenever a person with knowledge of the password changes to a role where they no longer require knowledge of the password (e.g., leaves the College or changes positions), the password must be changed.
- 6.6 Passwords for College systems must be unique.
 - a. Users should never use their College password for any third-party systems, even if used for College business purposes.
 - b. Users should never use the same password for privileged and non-privileged accounts.
- 6.7 Users must not store passwords for College systems in applications or browser password storage tools unless those tools use encrypted storage and the passwords meet College authentication standards.
 - a. The use of browser-based password managers (e.g., Chrome, Edge) is permitted if the device is secure, the storage is encrypted, and the password meets College security policies.
 - b. For higher-risk systems, such as those involving financial, HR, or student records, the College recommends using an IT-approved password manager that supports work/personal separation and secure backup. Contact IT for a list of approved tools and current recommendations.

7.00 ACCOUNT AND COMPUTER USE

- 7.1 Users must:
 - a. always log out of applications or lock computers when leaving a computer to prevent unauthorized use
 - b. not attempt to circumvent College-established authentication processes
 - c. follow IT standards for authentication and password specifications.

7.2 Authentication:

- a. All Users of accounts must protect any authentication mechanisms, including passwords or other authentication factors (e.g., MFA tokens, certificates, internet cookies) to ensure only appropriate access to College data and resources.

7.3 Policy:

- a. All Users of accounts must follow College policies and standards, including but not limited to:
 - i. [ADM-009, Student Non-Academic Conduct Policy](#)
 - ii. [INF-001, Acceptable Use of Information Systems Policy](#)
 - iii. [INF-002, Cybersecurity Policy](#)
 - iv. [HMR-001, Employee Code of Conduct](#)

7.4 Privileges:

- a. All accounts must be used only for the purpose for which they were authorized.

7.5 Misuse:

- a. Any disclosure of an account password or suspected compromise or misuse of accounts or data must be reported immediately to the IT Department (<https://cmtn.teamdynamix.com/>) or by telephone at 250.635.6511 Ext. 5999.

7.6 Accounts:

- a. All College business must be conducted using an account associated with @coastmountaincollege.ca addresses or approved exceptions.
- b. Non-College accounts such as personal Gmail and Yahoo accounts are not permitted to be used for conducting College business.
- c. To protect personal information, student, alumni, and retiree accounts must not be used for conducting College business.

7.7 Communication:

- a. Official College communications may be delivered to preferred or required addresses for those with @coastmountaincollege.ca addresses.
- b. Account holders must periodically check these accounts for required communication and, if forwarding is allowed, are responsible for checking the destination address.
- c. The College is not responsible for messages forwarded to third-party mailboxes.
- d. Some College business processes may require receiving messages from valid College email addresses and may not accept messages from third-party accounts (e.g., Gmail, Yahoo).

7.8 Third-Party Accounts:

- a. Accounts created in non-College systems but used for College business must be handled consistent with the policies for accounts, including association with @coastmountaincollege.ca email addresses, and the current standards published by IT.

8.00 RESPONSIBILITIES OF ACCOUNT MANAGERS

8.1 Authority:

- a. Managing accounts is the responsibility of IT.
- b. All accounts must be managed in accordance with current IT standards, including requirements for identity vetting, passwords, multifactor authentication, federation, auditing, and lifecycle (creation and termination).
- c. IT may publish standards to supplement and enforce this policy.

8.2 Automation:

- a. Automated account management (software and/or scripts) will be used to ensure that accounts are managed as appropriate when each account User's role with the College changes according to official College records.
- b. Use of all accounts will be monitored by automated tools to detect atypical use and ITS will take appropriate action, up to and including disabling the account.

8.3 Access:

- a. Access granted to each account must be reviewed at least annually by the appropriate data owner or account manager to ensure all access is authorized.

9.00 ACCOUNT MANAGEMENT

9.1 Shared Accounts:

- a. Shared accounts will not be created or assigned when an individual account access method is available. IT will approve the use of all shared accounts.

9.2 Inactive Accounts:

- a. Built-in or automated systems will disable any account that is determined to be inactive.
- b. Account inactivity timeframes will be determined according to risk and published as IT Department standards, but in no case should they exceed 180 days.
- c. Exceptions can be made for accounts which are not used interactively or where active use is not expected or cannot be accurately determined.

9.3 Lifecycle:

- a. All accounts will be maintained only if the account holder has a documented affiliation with the College.
- b. Accounts will not be created until there are sufficient records to uniquely identify the account holder.
- c. Changes to College roles of the account holder require a review of access granted to their accounts. This includes changing assigned access, up to and including account renaming or creation of a new account for the new role.

9.4 Auditing:

- a. Information systems used at the College must audit account creation, modification, enabling, disabling, and removal actions, and notify the account manager or security operations team and/or log centrally.

9.5 Federation:

- a. Federated identity services for College accounts will only be provided by IT or IT-approved systems or vendors.
- b. Federation will be used by all College applications and websites or for any service used by many faculty, staff, or students.

9.6 Preferred Email:

- a. Accounts and records will be maintained to enforce the use of @coastmountaincollege.ca email addresses for communication to employees or other approved individuals conducting College business. This includes publishing in the campus directory.
- b. Students, alumni, and retirees should use alternate domains or email addresses for personal or student matters to ensure their records are separate from College business that may be subject to public records requests.
- c. Active students, enrolled in the current term, must have their preferred email address set to their @coastmountaincollege.ca email address.
- d. Individuals with multiple roles should be assigned a preferred email address based upon their primary role.
- e. Where possible, use of student and employee addresses for communication should favour role-based official College addresses, rather than using the preferred address.

9.7 Auto-Forwarding Email:

- a. College systems will be configured to prevent automatic forwarding of email directly, or via rule or filter, for accounts created for the conduct of College business.
 - i. This does not apply to Students who are permitted to forward to their personal email accounts.
- b. Where it is not possible to prevent this configuration, automation will be used when possible to correct the automatic forwarding and notify the User of the change.
- c. Accounts not directly, or reasonably expected, to be involved in College business, including but not limited to students, alumni, and retirees, will be allowed to auto-forward email.

9.8 Account Reuse:

- a. Once an individual account has been assigned and used by a person, it will not be assigned or re-used by any other person. This includes both the specific account, and re-use of the email address at any future date.

9.9 Privileged Accounts:

- a. Separate individual accounts will be created and must be used for any privileged access.
 - i. Use of privileged accounts will be logged.
- b. Privileged accounts must not be used for non-privileged functions (e.g., email, web browsing).

- c. Staff with privileged access must perform day-to-day activities using a separate unprivileged account, and only use the privileged account when elevated access is explicitly required.

9.10 Passwords:

- a. All systems and accounts will be configured to require or meet current IT password standards.

9.11 Least Privilege:

- a. When provisioning accounts, principles of least privilege will apply.
- b. To the extent possible, accounts should be granted sufficient privileges to perform approved functions and no more.

10.00 REMEDIATION AND COMPLIANCE

- 10.1 Noncompliance with this policy will be considered a violation of [INF-001, Acceptable Use of Information Systems Policy](#) and will be addressed and remediated accordingly.

11.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

- 11.1 [ADM-009, Student Non-Academic Misconduct Policy](#)
- 11.2 [ADM-009P, Student Non-Academic Misconduct Procedure](#)
- 11.3 [HMR-001, Employee Code of Conduct](#)
- 11.4 [INF-001, Acceptable Use of Information Systems Policy](#)
- 11.5 [INF-002, Cybersecurity Policy](#)
- 11.6 [INF-002P, Cybersecurity Procedure](#)
- 11.7 *INF-004, IT Password and Authentication Policy*
- 11.8 *INF-004G, IT Password Management Guideline*

12.00 OTHER SUPPORTING DOCUMENTS

- 12.1 [BC Freedom of Information and Protection of Privacy Act](#)
- 12.2 [COBIT DSS05.02 Manage Network and Connectivity Security](#)
- 12.3 [Cybersecurity Framework | NIST](#)

13.00 HISTORY

Created/Revised/ Reviewed	Date	Author's Name and Role	Approved By
Created	Sept. 5, 2025	Director, Information Technology/CIO	President's Council & Board of Governors