


Policy Name:	USER ACCOUNT MANAGEMENT	
Approved By:	President's Council & Board of Governors	
Approval Date:	Sept. 5, 2025	
Next Scheduled Renewal Date:	August 2030	
Policy Holder:	VP, Corporate Services & CFO	
Operational Lead:	Director, Information Technology/CIO	
Policy Number:	INF-003	

## USER ACCOUNT MANAGEMENT POLICY

### 1.00 PURPOSE

- 1.1 The purpose of this policy is to establish a framework for managing User accounts at Coast Mountain College (the College) to ensure appropriate access, security, and accountability for information systems.

### 2.00 DEFINITIONS

- 2.1 **Account:** For purposes of this policy, 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 Types:
  - 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 College 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:** Accounts 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.

- 2.3 **Data Owner:** Typically a department head or senior staff member responsible for data primarily used or stored within their functional area. The data owner is accountable for the classification of data, approving access, and conducting periodic reviews to ensure the classification remains appropriate.
- 2.4 **Employee:** Any person employed by the College and, within the application of this policy, including members of the Board of Governors.
- 2.5 **Information Technology (IT):** For the purposes of this procedure, IT refers to the Information Technology Department.
- 2.6 **Role-Based Access Control (RBAC):** An approach to restricting system access to authorized Users, and to implementing mandatory access control or discretionary access control.
- 2.7 **Student:** An individual who is registered in a course or program at the College, including individuals registered in a course or program as a result of a partnership (e.g., dual credit).
- 2.8 **The College:** Coast Mountain College (CMTN).

### 3.00 SCOPE

- 3.1 This policy applies to all employees, students, contractors, suppliers, and consultants who require access to the College's information systems.
- 3.2 This policy should be read in conjunction with INF-004, *IT Password and Authentication Policy* for authentication-related requirements and [INF-001, Acceptable Use of College Information Technology Policy](#) for acceptable use guidelines.

### 4.00 ACCOUNT PROVISIONING AND ACCESS MANAGEMENT

- 4.1 User accounts are created based on role-based access control (RBAC) principles, ensuring least-privilege access.
- 4.2 Accounts will only be issued to authorized individuals with a legitimate academic, administrative, or business need.
- 4.3 Data owners (e.g., department heads) must approve account access requests for their respective systems.
- 4.4 System service accounts required for software performance will be managed by IT and restricted to necessary functions only.
- 4.5 Requests for temporary access or privileged access require IT review and approval.

## 5.00 ACCOUNT REVIEWS AND DEACTIVATION

- 5.1 Accounts will automatically be deactivated on their owner's last scheduled day of work.
  - a. An offboarding request will need to be completed by the department manager, delegate (e.g., an executive assistant or administrative assistant) or Human Resources and forwarded to IT.
- 5.2 Employees who are on long term disability with a scheduled return date will have all local access suspended but may continue to have access to College email and access to myCMTN upon the request of their manager or Human Resources.
- 5.3 Employees on permanent disability will have all access revoked and Human Resources will complete an offboarding request upon receiving notification of the employee's status.
- 5.4 All User accounts must be periodically reviewed to ensure appropriate access levels:
  - a. Quarterly review: Data owners must verify that active accounts have the correct permissions.
  - b. Monthly audit: IT must identify and flag inactive accounts.
- 5.5 Inactive account management:
  - a. Employees who are inactive for 90 days will have their accounts suspended.
  - b. Students who are inactive for 160 days will have local access revoked.
  - c. All accounts that are inactive for 365 days will have remote access disabled.
- 5.6 IT will notify account Users of any upcoming account disablement through their official College email.
- 5.7 Expired and disabled accounts will be permanently deleted within two years unless data retention policies require a longer retention period.
  - d. The User's department manager must request that the account data be retained beyond the two-year normal retention period.
  - e. Data from disabled accounts will be retained based on [ADM-011, Records Management Policy](#).

## 6.00 SECURITY AND COMPLIANCE REQUIREMENTS

- 6.1 In certain cases, User accounts may be activated prior to an employee's official start date to support project setup.
  - a. These exceptions must be requested by the Department Manager and approved by IT.
- 6.2 Temporary access extensions of up to five business days may be requested for departing employees or contractors in low-risk scenarios.
  - a. These requests must be approved by IT and the Vice President, Corporate Services & Chief Financial Officer (CFO).
- 6.3 Contractor and guest accounts must include defined expiration dates to ensure automatic access revocation upon the conclusion of the contract terms.

- 6.4 Requests for access that exceed the defined limits require approval from the Director of IT & Chief Information Officer (CIO) and the Vice President, Corporate Services & CFO.

7.00 ENFORCEMENT AND SANCTIONS

- 7.1 Violations may result in disciplinary action, including suspension of User account access, or legal action in the event of criminal activity.
- 7.2 Users found in violation of this policy will be subject to:
- a. investigation under applicable College policies and collective agreements; the investigation will be handled by the Human Resources Department
  - b. contract termination or cancellation for contractors and vendors.
- 7.3 System administrators may immediately revoke access if a security risk is detected.

8.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

- 8.1 [ADM-009, Student Non-Academic Conduct Policy](#)
- 8.2 [ADM-011, Records Management Policy](#)
- 8.3 [HMR-001, Employee Code of Conduct](#)
- 8.4 [HMR-011, Information Security Awareness and Training Policy](#)
- 8.5 [INF-001, Acceptable Use of Information Technology Policy](#)
- 8.6 [INF-002, Cybersecurity Policy](#)
- 8.7 [INF-002P, Cybersecurity Procedure](#)
- 8.8 INF-004, *IT Password and Authentication Policy*
- 8.9 INF-004P, *IT Password and Authentication Procedure*
- 8.10 INF-005, *Data Classification Policy*
- 8.11 INF-005P, *Data Classification Procedure*

9.00 OTHER SUPPORTING DOCUMENTS

- 9.1 [British Columbia Freedom of Information and Protection of Privacy Act](#) (FOIPPA BC)
- 9.2 [Criminal Code of Canada](#)

10.00 HISTORY

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