


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

## IT PASSWORD AND AUTHENTICATION POLICY

### 1.00 PURPOSE

- 1.1 The purpose of this policy is to establish a standard for the means of authenticating access to Coast Mountain College (the College; CMTN) resources.

### 2.00 DEFINITIONS

The following definitions apply in this policy:

#### 2.1 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 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:** 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.

- 2.2 **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 identifier, like a fingerprint).
- 2.3 **Information Technology (IT):** For the purpose of this policy, IT refers to the Information Technology Department.
- 2.4 **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 passphrases.
- 2.5 **Systems Owner:** The Dean, Director, or Manager of a department that controls and is the main user of that system.
- 2.6 **The College:** Coast Mountain College (CMTN).
- 2.7 **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 POLICY STATEMENT

- 3.1 The College will work to ensure the safeguarding of personal and confidential information of all individuals and organizations affiliated with the institution.
- 3.2 College system Users will be required to choose passwords that assist in the control of access to systems and data.
- 3.3 Consistent with the College's requirements for identity and access management, Users must protect the integrity of their authentication methods.
- 3.4 The College will provide the appropriate level of security for systems based on the level of risk.
- 3.5 The College will provide access to systems and data in a way that such access can be audited and uniquely tied to the individual and their role.

### 4.00 GUIDING PRINCIPLES

- 4.1 Management approval is on file for the specific system access granted to every individual.
- 4.2 Only personnel authorized to access the computer system, network, or servers are granted access.
- 4.3 Where possible, all activity on the system, network, or servers may be traced to an individual.

- 4.4 User authentication passwords are kept securely.
- 4.5 An individual may be held accountable for all activity logged against their user identifier.

5.00 EXCEPTIONS

- 5.1 Exceptions to this policy may be submitted to the Systems Owner in writing.
- 5.2 If approved, the Systems Owner will forward the request to the Director of Information Technology/Chief Information Officer (CIO), who will assess the risk and make a recommendation to the Vice-President, Corporate Services & Chief Financial Officer (CFO).
- 5.3 Exceptions must be reviewed for reauthorization no less than annually.

6.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

- 6.1 [INF-001, Acceptable Use of Information Systems Policy](#)
- 6.2 [INF-002, Cybersecurity Policy](#)
- 6.3 [INF-002P, Cybersecurity Procedure](#)
- 6.4 INF-004P, *IT Password and Authentication Procedure*
- 6.5 Information and Communication Technology Usage Policy (under development)
- 6.6 Information Technology System Owner Policy (under development)
- 6.7 Password Management Guideline

7.00 OTHER SUPPORTING DOCUMENTS

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

8.00 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