


Policy Name:	CYBERSECURITY POLICY	
Approved By:	President's Council and Board of Governors	
Approval Date:	June 10, 2025	
Next Scheduled Renewal Date:	May 2030	
Policy Holder:	VP, Corporate Services and CFO	
Operational Lead:	Director, Information Technology/CIO	
Policy Number:	INF-002	

## CYBERSECURITY POLICY

### 1.00 PURPOSE

- 1.1 The purpose of this policy is to provide information about security breaches of personal information, health information, sensitive and confidential information, or research records, and outline the steps necessary to identify, contain, investigate, assess, analyze, report, and notify in the event of a breach.

### 2.00 DEFINITIONS

- 2.1 **Breach of Security Safeguards:** Unauthorized access, disclosure, or loss of personal information under the College's control due to cybersecurity failures.
- 2.2 **CFO:** Chief Financial Officer
- 2.3 **CIO:** Chief Information Officer
- 2.4 **Cybersecurity:** The practice of protecting systems, networks, and programs from digital attacks.
- 2.5 **Director:** Director, Information Technology & CIO
- 2.6 **Employee:** Any person employed by the College and, within the application of this policy, including members of the Board of Governors.
- 2.7 **Personal Information:** Any information relating to an identifiable individual, including names, contact details, financial information, medical records, and more, as defined under BC's [Freedom of Information and Protection of Privacy Act](#) (FOIPPA). Business contact information is excluded when the information is being used for business purposes.
- 2.8 **Privacy Officer:** The senior official designated to investigate disclosures of security breaches.
- 2.9 **Real Risk of Significant Harm (RRSH):** The likelihood of harm resulting from a breach, including financial loss, identity theft, reputational damage, and other significant impacts.

2.10 **Security Response Team (SRT):** A multidisciplinary group responsible for managing, coordinating, and responding to information security incidents and breaches. The group will be activated by the CIO in the event of a significant breach or incident.

2.11 **The College:** Coast Mountain College (CMTN).

### 3.00 POLICY STATEMENT

3.1 Coast Mountain College, as a public body under the BC [Freedom of Information and Protection of Privacy Act](#) (FOIPPA), must protect personal information, health information, sensitive or confidential information, and research records under its custody or control against such risks as unauthorized access, collection, use, disclosure, or destruction.

- a. As per FOIPPA data residency requirements, personal information must be stored and accessed only in Canada unless explicit consent is obtained or certain legal exceptions apply.
- b. Business information is not considered as personal information when being used for business purposes.

3.2 Through the course of its business, service, and research functions, the College may, with permission, gain access to health information as defined under applicable BC health information regulations. In such relationships, the College must also protect this information against unauthorized access, collection, use, disclosure, or destruction in accordance with relevant legislation.

### 4.00 GUIDING PRINCIPLES

4.1 The College will take all reasonable steps to maintain the confidentiality of College data and personal information under its control by developing and implementing policies and procedures to address any breach of security safeguards (i.e., security breach).

4.2 This policy applies to all employees, as well as suppliers and consultants providing goods and services to the College, and is applicable whenever there is a proven or suspected security breach.

### 5.00 EMPLOYEE TRAINING AND AWARENESS

5.1 The College is committed to ensuring that all employees are educated about their responsibilities for protecting personal and sensitive information.

5.2 Regular required training and awareness programs will be conducted for all staff to help them:

- a. recognize potential security threats, including phishing and social engineering attacks. Employees may be directed to additional training if required
- b. understand proper handling of personal, sensitive, and confidential information
- c. report suspicious activities and potential security breaches promptly
- d. comply with data protection laws such as BC's [Freedom of Information and Protection of Privacy Act](#) (FOIPPA).

5.3 All employees must complete mandatory annual data protection and security awareness training.

- 5.4 Specialized training may be required of staff who manage high-risk data or are part of the Security Response Team (SRT).

#### 6.00 MALWARE PREVENTION AND PROTECTION

- 6.1 All College-owned devices must have up-to-date antivirus and anti-malware software installed and managed by the Information Technology (IT) Department.
- 6.2 Users must not disable, bypass, or uninstall antivirus protections without IT authorization.
- 6.3 All employees must avoid downloading or installing unauthorized software.
- 6.4 Users must exercise caution when opening email attachments, links, and external files to prevent malware infections.

#### 7.00 REPORTING MALWARE INFECTIONS

- 7.1 If a device is suspected of being infected with malware, users must take the follow steps:
  - a. Disconnect from the network immediately.
  - b. Report the incident to IT for assessment and mitigation.
  - c. Follow IT's guidance for malware removal and security updates.
  - d. For malware incidents leading to a data breach, users must follow INF-002P, *Cybersecurity Procedure* for proper incident reporting and containment.

#### 8.00 NETWORK SECURITY AND PERSONAL DEVICE RESTRICTIONS

- 8.1 All devices connecting to the College's network must meet security compliance standards.
- 8.2 At the sole discretion of the College, personal devices may be restricted from accessing the public Wi-Fi network if they lack critical security updates, do not have adequate malware protection, or are detected as a security risk.
- 8.3 Personal devices must not be connected to the College-wired network without the prior approval of the Director.
- 8.4 Users must not engage in unauthorized network monitoring, scanning, or penetration testing.

#### 9.00 DATA LOSS PREVENTION (DLP) AND DATA SECURITY MEASURES

- 9.1 Sensitive College data must not be stored, transferred, or shared through unauthorized means.
- 9.2 DLP controls will be implemented by IT to monitor and prevent unauthorized data transfers.
- 9.3 Employees are prohibited from:
  - a. sending sensitive College data via personal email accounts or unauthorized cloud services
  - b. copying confidential College data to unencrypted USB devices; only IT-approved encrypted USB devices (e.g., BitLocker-encrypted drives with AES-256) may be used for secure storage and transfer

c. using unsecured file-sharing platforms that do not meet College security standards.

9.4 For all detected violations, the Director will initiate an investigation and appropriate corrective actions will be taken.

10.00 INCIDENT RESPONSE AND SECURITY BREACH HANDLING

10.1 When a security incident is suspected, it must be handled in accordance with INF-002P, *Cybersecurity Procedure*.

10.2 All breaches must be assessed for real risk of significant harm (RRSH).

10.3 Where required, the Privacy Officer must notify the Office of the Information and Privacy Commissioner (OIPC) as per FOIPPA requirements.

10.4 Post-incident reviews will be conducted to ensure continuous improvement in cybersecurity practices.

11.00 COMPLIANCE AND ENFORCEMENT

11.1 Users must comply with all relevant cybersecurity policies.

12.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

12.1 [ADM-003 Freedom of Information and Privacy Policy](#)

12.2 [ADM-011, Records Management Policy](#)

12.3 [HMR-011, Information Security Awareness and Training Policy](#)

12.4 [INF-001, Acceptable Use of Information Resources Policy](#)

12.5 INF-002P, *Cybersecurity Procedure*

12.6 INF-003, *User Account Management Policy*

12.7 INF-004, *IT Password and Authentication Policy*

12.8 INF-005, *College Data Classification Policy*

13.00 OTHER SUPPORTING DOCUMENTS

13.1 BC [Freedom of Information and Protection of Privacy Act](#) (FOIPPA), including data residency requirements

13.2 BC [Personal Health Information Protection Act](#) (PHIPA)

14.00 HISTORY

Created/Revised/Reviewed	Date	Author's Name and Role	Approved By
Created	June 10, 2025	Director, Information Technology/CIO	Board of Governors