


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

CYBERSECURITY PROCEDURE

1.00 PURPOSE

- 1.1 The purpose of this procedure is to outline how Coast Mountain College (CMTN) will respond in the event of a cybersecurity 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 **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.
- 2.7 **Privacy Officer:** The senior official designated to investigate disclosures of security breaches.
- 2.8 **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.
- 2.9 **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.
- 2.10 **The College:** Coast Mountain College (CMTN).

3.00 RESPONSIBILITIES

- 3.1 The Director will ensure that the IT Department develops, maintains, and tests appropriate policies and procedures to manage cybersecurity breaches, ensuring compliance with applicable laws and best practices, including BC's [Freedom of Information and Protection of Privacy Act](#) (FOIPPA).
- 3.2 All College personnel are responsible for complying with established security safeguards. If a necessary security safeguard has not yet been implemented, personnel must take actions to minimize the likelihood and impact of a potential cybersecurity breach.
- 3.3 The Director will establish an Information Technology Security Response Team (SRT), which must include appropriate representation from College units such as:
 - a. Information Technology (IT)
 - b. Human Resources
 - c. Finance
 - d. Communications and Marketing
 - e. Risk Management
 - f. VP, Corporate Services & CFO
 - g. Privacy Officer.
- 3.4 External participants may include external legal counsel, IT experts, insurance company representatives, and public relations firms.
- 3.5 The Director is responsible for leading cybersecurity breach protocols upon learning of a breach.
 - a. The SRT will assist in mobilizing the security breach protocols.
 - b. Delegation of responsibilities within the SRT may occur, but accountability remains with the Director.

4.00 SECURITY RESPONSE TEAM TRAINING

- 4.1 The SRT will receive specialized training focused on:
 - a. the data breach response procedure
 - b. technical skills necessary for breach containment and mitigation
 - c. legal obligations surrounding breach notification (e.g., when and how to notify regulatory bodies and affected individuals)
 - d. collaboration with external partners (e.g., legal counsel, cybersecurity firms, and law enforcement)
 - e. annual breach simulations and tabletop exercises to test the team's readiness and improve coordination during a real incident.
- 4.2 This training will be reviewed and, if necessary, updated and tested annually to ensure the team is prepared for evolving cybersecurity threats and can act quickly and effectively in the event of a breach.

5.00 COORDINATING COMMUNICATIONS

- 5.1 The SRT will ensure proper coordination of all internal and external communications related to the breach. This includes:
 - a. managing communications with affected individuals
 - b. ensuring timely reporting to regulatory bodies (e.g., Office of the Information and Privacy Commissioner [OIPC])
 - c. coordinating with external partners (e.g., cybersecurity firms, legal counsel)
 - d. communicating with media or the public, as necessary, to ensure consistent messaging and avoid reputational damage.
- 5.2 The Communications and Marketing Department within the SRT will take the lead in developing clear, consistent, and accurate communications in coordination with the VP, Corporate Services & CFO and other relevant team members.

6.00 SECURITY BREACH DISCOVERY

- 6.1 Immediate Notification:
 - a. Upon discovering a security breach, College personnel must immediately alert their manager or supervisor and the Director.
- 6.2 Confirmation and Activation:
 - a. The Director must make every effort to confirm the breach within 24 hours of notification.
 - i. If the breach cannot reasonably be confirmed within this period due to complexity or investigation requirements, the Director will update senior leadership and proceed with a detailed investigation to confirm the breach as soon as possible.
 - b. Once confirmed, the Director will advise the VP, Corporate Services & CFO and activate the cybersecurity breach protocols to ensure:
 - i. containment of the breach
 - ii. completion of risk assessments and investigations (Appendix C)
 - iii. reporting and notification to affected individuals and relevant third parties, as necessary
 - iv. implementation of long-term preventative or remedial strategies
 - v. documentation in the cybersecurity incident log (Appendix B)
 - vi. completion of the privacy or information cybersecurity breach reporting form (Appendix A).
- 6.3 Insurance Notification (if policy is in place):
 - a. The Director will inform the cybersecurity insurance provider of the potential breach, as per the claim reporting procedure.

7.00 CONTAINING THE BREACH

- 7.1 Upon breach confirmation, the Director will ensure that the appropriate personnel mitigate the breach's impact by:
- a. recovering compromised data, shutting down networks, remotely wiping devices, or stopping unauthorized practices
 - b. through the guidance of legal counsel, notifying law enforcement if the breach could involve criminal activity
 - c. mobilizing the SRT within 24 hours
 - d. ensuring all details of the breach remain confidential
 - e. engaging external cybersecurity experts if required to assist with containment efforts and ensure that all potential vulnerabilities are addressed effectively.

8.00 RISK ASSESSMENTS AND INVESTIGATIONS

- 8.1 The Director will lead investigations and risk assessments to determine whether the breach poses a real risk of significant harm.
- a. This includes assessing the sensitivity of compromised information and the probability of misuse, with preliminary assessments completed within 24 hours and in-depth investigations as required.
- 8.2 Evaluation by the SRT:
- a. The SRT will evaluate:
 - i. the sensitivity of the compromised information
 - ii. the probability of misuse and potential for harm (e.g., identity theft, reputational damage)
 - iii. other factors required under applicable privacy laws.
- 8.3 Notifications by the VP, Corporate Services & CFO:
- a. If a real risk of significant harm is identified, the VP, Corporate Services & CFO will notify:
 - i. the President, who will inform the Board Chair of the breach if it is deemed significant or likely to have broader implications for the institution
 - ii. the Ministry of Post-Secondary Education and Future Skills.
- 8.4 Notifications by the Privacy Officer:
- a. If a real risk of significant harm is identified by the VP, Corporate Services & CFO, the Privacy Officer will notify:
 - i. affected individuals
 - ii. the Office of the Information and Privacy (OIPC) Commissioner of BC, if required by FOIPPA.
- 8.5 Reporting to OIPC:
- a. The Privacy Officer will ensure that the report includes details of the breach and mitigation efforts and is submitted to OIPC as required by FOIPPA.

8.6 Additional Notifications:

- a. The Director, VP, Corporate Services & CFO, and Privacy Officer will consider whether additional notifications are necessary, including to insurers, legal counsel, business partners, and possibly the general public.

8.7 Post-Incident Review:

- a. Once the breach has been resolved, the SRT will conduct a post-incident review to assess the effectiveness of the breach response.
 - i. The review should identify lessons learned, recommend improvements to breach management processes, and suggest actions to prevent future breaches.
 - ii. The review should be documented and presented to senior leadership, including the Board Chair, as appropriate.

9.00 REMEDIAL ACTIONS AND PREVENTATIVE STRATEGIES

9.1 After containing the breach, the Director must:

- a. implement remedial actions, such as additional training or changes to business practices
- b. enhance technological safeguards based on the breach's nature
- c. log the incident in the cybersecurity incident log maintained by the Director
- d. provide the Privacy Officer with a report to OIPC with a copy of the final breach report (Appendix A)
- e. conduct a post-incident review to evaluate the efficacy of breach response protocols and implement improvements based on lessons learned.

10.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

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

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

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

11.00 OTHER SUPPORTING DOCUMENTS

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

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

11.3 Canadian [Personal Information Protection and Electronic Documents Act](#) (PIPEDA)

HISTORY

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

Appendix A: Privacy or Information Security Breach Reporting Form

In the event of a breach, the College must report to the Office of the Information and Privacy Commissioner for BC (OIPC). The breach reporting form can be completed on the OIPC website:

[Online Privacy Breach Report Form - OIPC](#)

Organizations are required to submit the completed form as part of their breach reporting obligations under FOIPPA.

Appendix B: Cybersecurity Incident Log Template

The example below shows the type of information collected in the CMTN cybersecurity incident log. This log will be maintained by the Director.

Incident ID	Date of Incident	Date Reported	Breach Description	Data Compromised	Individuals Affected	Containment Measures	Risk Assessment Completed	Notifications Sent	Date Resolved	Remedial Actions	Post-Incident Review Date	Comments/Notes
Incident-001	2024-01-10	2024-01-11	Unauthorized access to HR files	Employee personal data	50 employees	Systems isolated, access revoked	Yes	Affected individuals, OIPC	2024-01-13	Security audit performed, passwords reset	2024-01-20	
Incident-002	2024-02-25	2024-02-26	Phishing attack, email compromise	Student data	150 students	Emails blocked, accounts frozen	Yes	Affected individuals	2024-02-28	Anti-phishing training implemented	2024-03-05	
...	

Appendix C: Cybersecurity Risk Template

This form is used by the Director to document risk assessments and investigations.

Risk Impact	Date Identified	Description of Risk	Likelihood (L, M, H) ¹	Impact (L, M, H) ¹	Risk Level (Overall)	Mitigation Strategy	Responsible Party	Resolution Deadline	Status (O, C) ²	Comments/Notes
1. Low, Medium, High 2. Open, Closed										