Policy Name:	INFORMATION SECURITY AWARENESS AND TRAINING
Approved By:	President's Council
Approval Date:	March 8, 2022
Next Scheduled Renewal Date:	February 2027
Policy Holder:	VP, Corporate Services
Operational Lead:	Director, Human Resources
Policy Number:	HMR-011

INFORMATION SECURITY AWARENESS AND TRAINING POLICY

1.00 PURPOSE

1.1 The purpose of this policy is to establish appropriate risk mitigation in ensuring awareness and training of Coast Mountain College (CMTN) employees against growing trends of social engineering attacks and frauds.

1.2 It is also to ensure that College employees and affiliates with access to College data have an adequate level of understanding for the importance of securing institutional data and information resources.

2.00 DEFINITIONS

2.1 **College Affiliate or Contractor**: Someone officially attached or connected to the College who is not a student or employee.

2.2 **Employee**: Any person employed by the College, including part-time, term and student employees.

2.3 **Information Resources**: Any devices, assets, and infrastructure owned by, explicitly controlled by, or in the custody of the College, including but not limited to data, records, electronic services, network services, software, computers, laptops, tablets, smartphones, mobile computing devices, and information systems.

2.4 **Information Security Awareness Training**: A formal process for educating employees about the best practices to follow while using institutional information resources in consideration with information security.

3.00 SCOPE

3.1 This policy applies to all CMTN staff and faculty members, referred to as employees hereafter.

3.2 Other members of the College (students, alumni, etc.) are encouraged to participate in our various cybersecurity training and awareness opportunities when offered, but compliance with this policy will not be enforced for non-employees other than the exceptions stated in 3.3 and 3.4.

3.3 This policy applies to the employed members of Coast Mountain College Student Union having access to College's information resources and the students who have a role as part-time or full-time employees of the College.

3.4 This policy also applies to third-party employees (contractors, consultants) working for the College, whether they are explicitly bound (e.g., by contractual terms and conditions) or implicitly bound (e.g., by generally held standards of ethics and acceptable behaviour) and have access to College's information resources.

4.00 COMPLIANCE

4.1 Information security is vital in today's environment; consequently, CMTN requires that all employees participate in our information security program.

4.2 Failure to comply with this policy may result in changes to or limits on the individual's network access, in consultation with the Senior Manager responsible for the department, disciplinary action, and/or up to termination.

4.3 Disciplinary action follows established College policies and procedures and will be in accordance with the applicable handbook, collective agreement, and/or employee manual.

5.00 POLICY STATEMENTS

5.1 College Employees will be required to complete a mandatory information security awareness training course upon accepting an employment with the College and must finish within the first 30 days of the employment.

5.2 Employees will be required to review and complete the training/basic security courses again as part of comprehensive information security program annually.

a) As information security threats evolve, content of the training will vary every year.

b) Certain employees may be required to complete additional role-specific training depending on their job requirements.

c) An employee will be given a reasonable amount of time (up to 30 days) to complete training so as to not disrupt business operations.

5.3 This and any subsequent training must occur within regularly scheduled work hours and is considered part of the employee's work responsibilities.

a) Current employees must engage in this training within 30 days of approval of this policy by President's Council.

5.4 College Employees will be included in phishing awareness and social engineering training exercises.

a) These exercises will comprise a deceptive email being sent to each employee at random times throughout the year.

b) Moreover, it may include other means of phishing such as vishing (voice), smishing (SMS), USB testing and physical assessments.

c) Employees should simply delete the emails/SMS and/or report it to the Information Technology Department through the PhishALERT button or a service-desk ticket.

d) Those that interact with the phishing email (i.e., repeatedly clicking on links, entering credentials, downloading attachments or sharing College information to un-

authorized person) will be enrolled in a short supplementary cybersecurity training course to educate them how to recognize and avoid future attacks.

e) Completion of this training is mandatory and failure to comply will be reported to the Employee's Supervisor.

f) Employees will have 10 business days to complete the training with each simulation failure that occurs.

5.5 The analytics of an Employee's compliance with the policy will be monitored by the College's Information Technology Department and shared with Individual Employees as well as the team of Executives.

5.6 The employee's enrolment and completion of the training will be monitored by the Information Technology Department and may be shared with the Senior Manager of the respective department and/or Team of Executives.

6.00 RELATED POLICIES AND PROCEDURES

6.1 ADM-007, *Acceptable Use of Information Resources*

6.2 ADM-011, *Records Management*

6.3 HMR-001, *Employee Code of Conduct*

7.00 OTHER SUPPORTING DOCUMENTS

7.1 CUPE 2409/FPSE 11 Collective Agreement & FPSE Common Agreement

7.2 BCGEU Local 712 Instructor Collective Agreement & BCGEU Common Agreement

7.3 BCGEU Local 712 Support Staff Collective Agreement

7.4 Excluded Staff Employment Agreements

8.00 HISTORY

Created/Revised/ Reviewed	Date	Author's Name and Role	Approved By
Created			