Procedure Name:	Information Security Awareness and Training Procedures
Approval Date:	
Procedure Holder:	VP Corporate Services
Procedure Number:	HR – 11P

coast mountain college

INFORMATION SECURITY AWARENESS AND TRAINING PROCEDURES

1.0 PHISHING AWARENESS AND SOCIAL ENGINEERING EXERCISES

1.01 The College's IT department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The College's IT department will conduct these tests at random throughout the year with no set schedule or frequency. The College's IT department may conduct targeted exercises against specific departments.

1.02 The Information Technology department will craft deceptive simulated phishing email that may include an attachment and/or link, deliver the email to a set of end-users (employees or department). Employees should delete the emails/SMS and/or report it to the Information Technology department through the PhishALERT button or a service-desk ticket.

1.03 Similarly, employees may receive a phone call onto their extension and/or SMS to college provided cell-phone to request sensitive information. End-users should not share any information to an unknown entity.

2.0 ADDITIONAL ROLE SPECIFIC TRAINING

2.01 Employees having access to sensitive information would be required to enroll in additional role-specific training. This training is appropriate for staff with specific obligations towards information security in their role that are not satisfied by basic security awareness, which includes but is not limited to Information Risk and Security Management, IT/Network Operations personnel, Payroll, HR, Finance, Registration and more.

2.02 Where necessary and practicable, Information security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for employees focused on their job functions and broader responsibilities at the college. For example, an employee accessing information which is sensitive in nature (for e.g. student's personal information, SIN) would be required to enroll in the training on how to handle information which is related to someone's privacy.

2.03 The following is a list of example situations that may require an increased sophistication of information security awareness training and respective exercises.

2.03.1 Employee is a high value target

2.03.2 Employee has access to sensitive information

2.03.3 Employee has access to College information resources which are valued to be confidential or highly restricted

2.03.4 Employee maintains weak security practices (example: not having strong passwords, store passwords onto a clear text file and many more)

2.03.5 Employee has repeated organizational policy violations about privacy

3.0 COMPLIANCE AND NON-COMPLIANCE ACTIONS

3.01 Certain actions or non-actions by college employee may result in a compliance event (Pass). A Pass includes but is not limited to,

3.01.1 Successfully identifying a simulated social engineering exercise

3.01.2 Not having a Failure during a social engineering exercise (Non-action)

3.01.3 Reporting real social engineering attacks to the IT department

3.02 Certain actions or non-actions by the college employee may result in a non-compliance event (Failure). A Failure includes but is not limited to,

3.02.1 Failure to complete required training within the time allotted

3.02.2 Failure of a social engineering exercise

3.03 Failure of a social engineering exercise includes but is not limited to:

3.03.1 Clicking on a URL within a phishing test

3.03.2 Replying with any information to a phishing test

3.03.3 Opening an attachment that is part of a phishing test

3.03.4 Enabling macros that are within an attachment as part of a phishing test

3.03.5 Allowing exploit code to run as part of a phishing test

3.03.6 Entering any data within a landing page as part of a phishing test

3.03.7 Transmitting any information as part of a vishing test

3.03.8 Replying with any information to a smishing test

3.03.9 Plugging in a USB stick or removable drive as part of a social engineering exercise

3.03.10 Failing to follow organization policies in the course of a physical social engineering exercise

4.0 COMPLIANCE REPORTING AND ESCALATIONS

4.01 The Information Technology department follows the principle of least privileges. Only a few individuals from the Information Technology department including the Senior Cybersecurity Architect, Information Security Analysts and Director of Information Technology will have access to monitor the employee’s actions over simulated phishing awareness exercises.

4.02 Moreover, the analytics would be shared with the employee’s supervisors and/or department head to provide information on compliance with the policy in regards to success/failure attempts to the phishing awareness exercises and/or completion of required training within the allotted time. The employee’s supervisor and/or department head would be consulted for any escalations if required.

4.03 These consolidated analytics would be shared with the team of Executives (including VPs and President) so that they would be aware about organization wide security and threat landscape and can make informed decisions. In the event of any disciplinary actions, such analytics would be shared with HR and/or union representatives.

5.0 NOTIFICATIONS

5.01 Employees will receive the training notification through their college email address.

5.02 Information Technology department will send the reminders for completion of required trainings.

5.03 Any escalations to employee’s supervisor and/department head will be sent over college email.