Procedure Name:	INFORMATION SECURITY AWARENESS AND TRAINING
Approved By:	President's Council
Approval Date:	March 8, 2022
Next Scheduled Renewal Date:	February 2027
Procedure Holder:	VP, Corporate Services
Operational Lead:	Manager, IT Infrastructure
Procedure Number:	HMR-011P

INFORMATION SECURITY AWARENESS AND TRAINING PROCEDURE

1.00 PURPOSE

1.1 This procedure outlines the steps to be taken when implementing information security awareness and training, including role-specific training, and compliance and non-compliance actions.

2.00 DEFINITIONS

2.1 None

3.00 PHISHING AWARENESS AND SOCIAL ENGINEERING EXERCISES

3.1 The College’s Information Technology (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.

3.2 The College’s IT Department:

a) will conduct these tests at random throughout the year with no set schedule or frequency

b) may conduct targeted exercises against specific departments.

3.3 The IT Department will craft deceptive simulated phishing emails that may include an attachment and/or link, deliver the email to a set of end-users (employees or department).

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

3.4 Similarly, employees may receive a phone call on their extension and/or SMS to College-provided cell-phone to request sensitive information.

a) End-users should not share any information with an unknown entity.

4.00 ADDITIONAL ROLE-SPECIFIC TRAINING

4.1 Employees having access to sensitive information will be required to enroll in additional role-specific training.

4.2 Role-specific 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:

a) Information Risk and Security Management

b) IT/Network Operations personnel

c) Payroll

d) Human Resources

e) Finance

f) Registration, and more.

4.3 Where necessary and practicable, information security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, and technical content.

a) 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 sensitive information (e.g., student's personal information, SIN) will be required to enroll in the training on how to handle information that is related to someone's privacy.

4.4 Situations that may require an increased sophistication of information security awareness training and respective exercises include those where the employee:

a) is a high value target

b) has access to sensitive information

c) has access to College information resources which are designated confidential or highly restricted

d) maintains weak security practices (e.g., not having strong passwords, storing passwords on a clear text file)

e) employee has repeated organizational policy violations about privacy.

5.00 COMPLIANCE AND NON-COMPLIANCE ACTIONS

5.1 Certain actions or non-actions by College employees may result in a compliance event (Pass). A Pass includes but is not limited to:

a) successfully identifying a simulated social engineering exercise

b) not having a Failure during a social engineering exercise (non-action)

c) reporting real social engineering attacks to the IT Department.

5.2 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 the failure:

a) to complete the required training within the time allotted

b) to successfully identify a social engineering exercise.

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

a) clicking on a URL in a phishing test

b) replying with any information to a phishing test

c) opening an attachment that is part of a phishing test

d) enabling macros that are within an attachment as part of a phishing test

e) allowing exploit code to run as part of a phishing test

f) entering any data within a landing page as part of a phishing test

g) transmitting any information as part of a vishing test

h) replying with any information to a smishing test

i) plugging in a USB stick or removable drive as part of a social engineering exercise

j) failing to follow organization policies in the course of a physical social engineering exercise.

6.00 COMPLIANCE REPORTING AND ESCALATIONS

6.1 The IT Department follows the principle of least privileges.

a) Only a few individuals from the IT 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.

6.2 The analytics will be shared with the employee’s supervisors and/or department head to provide information on compliance with the policy with regard to success or failure attempts to the phishing awareness exercises and/or completion of required training within the allotted time.

a) The employee’s supervisor and/or department head will be consulted for any escalations, if required.

6.3 These consolidated analytics will be shared with the team of executives (including VPs and President & CEO) so that they will be aware of the organization-wide security and threat landscape and can make informed decisions.

a) In the event of any disciplinary actions, such analytics will be shared with Human Resources and/or union representatives.

7.00 NOTIFICATIONS

7.1 Employees will receive the training notification through their College email address.

7.2 The IT Department will send the reminders for completion of required trainings.

7.3 Any escalations to the employee’s supervisor and/or department head will be sent over College email.

8.00 RELATED POLICIES, PROCEDURES, AND SUPPORTING DOCUMENTS

8.1 HMR-011, *Information Security Awareness Training Policy*

9.00 HISTORY

Created/Revised/ Reviewed	**Date**	**Author’s Name and Role**	**Approved By**
Created	March 8, 2022	Manager, IT Infrastructure	President’s Council