POLICY

CATEGORY	Administrative
POLICY NUMBER	**E07**
POLICY NAME	**Cyber Security Awareness Training**
CROSS REFERENCE	A25 Code of Conduct E02 ITM Privacy Information, Security and Identity Management Information and Technology Services Use Agreement

COLLEGE LEADERSHIP TEAM	**ACADEMIC COUNCIL**
March 21, 2019	

POLICY STATEMENT

Overview

People are the first and best line of defense for security. If individuals who require access to the Institution's resources understand the reason for security – the "why" – then they will be much more likely to adhere to security controls, and to enforce controls such as not disclosing passwords via a phishing email. If they understand the threats and risks – the "what" – and the measures to counter the threats and risks – the "how" – then they will help to create an effective security culture. To a very large extent, a strong security posture depends on the effectiveness of security awareness amongst all those contributing to the success of the Institution in achieving business objectives.

The protection of Institution information and assets depends on individuals – understanding their rights and responsibilities for the protection of Olds College's reputation and information assets.

Scope

Olds College will establish and maintain an information technology security awareness and training program to ensure that all College employees are aware of their security responsibilities in regards to College IT resources.

The objectives of the security awareness training:

- users will be able to recognize the risks and vulnerabilities facing the College environment
- users will know the tools they can use to minimize these risks and vulnerabilities

Standard Requirements

All College staff & faculty are required to participate in information technology security awareness training by utilizing an online service as arranged by the IT Department.

All new employees must complete the IT security awareness training as part of the orientation process within 30 days of their hire date.

- All employees are required to successfully complete the "Required Training" module each school year.
- Specifically tailored training modules can be made available for users' roles such as technically savvy IT Staff, Executive Leadership, Admin staff, Business Services staff, in addition to the basic training.
- Training delivery accommodations, such as group sessions, can also be made for staff that have limited access to computers.

The IT Department is responsible for:

1. Providing security awareness information to employees on a regular basis;
2. Reviewing and updating, as necessary, security awareness material on an annual basis;
3. Disseminating warning bulletins on new instances of malicious code or system attacks, as appropriate;
4. Maintaining a record of employees and contractors who have completed the securityawareness training.
5. Cyber Security Incident Management.

Security awareness materials will include:

- Identifying the importance of security to the Institution's sound operation and achievement of College objectives;
- Acceptable use of IT resources;
- Threats, vulnerabilities and risks: an overview of threat and risk assessment;
- Privacy requirements in accordance with legislation and an overview of Privacy ImpactAssessments;
- Security responsibilities of all employees including:
    - Protection of security technology and authentication mechanisms, such as passwords, PINs, access and/or ID cards, desktop rules such as locked screen saver;
    - Recognizing IT threats and preventing their realization: phishing, pharming, social engineering techniques, avoiding the introduction of malicious software from untrusted websites or portable media, etc.;

Compliance and Monitoring

- Each employee's completion of the training and the acknowledgement will be recordedelectronically.
- Reports about the completion status of individuals will be generated and provided to the HR department.
- Deans and Directors are responsible for ensuring that the employees who report to them complete this process.

IMPLEMENTATION AND ADMINISTRATIVE RESPONSIBILITY	
VICE PRESIDENT Responsible for:	Information Technology
Review Period	2 Years