Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Information Security
NO.:	ADMIN-276
RESPONSIBILITY:	Chief Administrative Officer and Associate Vice-President, Information Technology
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	September 2019
REVISED DATE(S):	
REVIEW DATE:	September 2022

1. Introduction

The Information Security Policy is the cornerstone of the College's information security program. It establishes the concept that Information is an asset and the property of Durham College. All Information Technology Users are required to protect this asset.

In securing Information, it is essential that the following characteristics of Information are preserved and maintained:

- Confidentiality: ensuring that Information is accessible only to those authorized to have access;
- Integrity: safeguarding the accuracy and completeness of Information and processing methods;
- Availability: ensuring that authorized users will have access to Information and associated assets when required.

2. Purpose

This policy establishes a framework for the security of the College's Information.

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

4.1. Scope

4.1.1. This policy applies to all Information within the custody and control of the College, including the Cardholder Data Environment (CDE). Any activity aimed at the manipulation, transportation or use of Information is subject to this policy throughout its life cycle.

4.1.2. This policy applies to all Information Technology Users having access, on-site or outside the physical locations of Durham College, to Information for which the College is responsible for ensuring the safety of the Information.

4.2. Information Owners are responsible for properly classifying assets in terms of their confidentiality, integrity and availability. Information needs to be classified and protected based on its risk profile as described in the Information Management Policy.

4.3. If there are several potential Information Owners for a particular information asset, DCLT will assign the information ownership to the most appropriate role at the College.

4.4. The following roles are the Information Owners of the respective information sets:

- DC Connect: Vice-President, Academic
- Banner Student: Associate Vice-President, Student Affairs and Registrar
- Banner HR: Associate Vice-President, Human Resources
- Banner Finance: Vice-President, Administration and Chief Financial Officer
- ICE: Associate Vice-President, Communications and Marketing

4.6. IT Services will be the Information Custodian of key services, such as DC Connect, Banner, ICE, e-mail and shared folders.

4.7. Information Owners and Information Custodians shall work together to ensure adequate access measures are in place to protect Information from loss or unauthorized access or inappropriate use.

4.8. Information Owners and Information Custodians shall work together to ensure the integrity of Information is maintained by protecting against unauthorized modification.

4.9. Information Owners and Information Custodians shall work together to protect confidential Information from unauthorized disclosure.

4.10. Information Technology Users may only have access to the confidential Information that is required to perform their roles. They shall protect the confidentiality of the Information to which they have access.

4.11. Information Owners and Information Custodians shall work together to ensure availability of Information of key services such as DC Connect, Banner, e-mail, ICE and shared storage drives is maintained.

4.12. Information security awareness materials will be available to all Employees.

4.13. Physical access to the IT Services data centre needs to be secured by two types of locks: a physical lock and a biometric scanning device. Employees and visitors that enter the data centre need to be tracked in a log book by staff from IT Services and Facilities authorized to enter the data centre.

4.14. An IT information security incident response plan needs to be in place, reviewed and tested.

4.15. All actual or suspected information security breaches must be reported to the Information Security Officer and will be investigated following the relevant steps in the Acceptable Use of Information Technology Policy and Procedure. Where relevant, a breach must be reported to the Privacy Officer.

5. Procedure

IT Services will maintain a set of departmental policies that reflects the information security practices for key services. The set will include the following departmental policies: Firewall Policy, Encryption Policy, Vulnerability Management and Information Security Incident Response Plan, and Backup Policy.

6. Roles and responsibilities

6.1. All Information Technology Users are in part responsible for protecting College Information from unauthorized access, modification, destruction or disclosure.

6.2. All Information Technology Users are accountable for complying with information security policies, and are responsible for the consequences of their actions regarding computing security practices.

6.3. Information Owners are responsible for properly classifying assets in terms of the confidentiality, integrity and availability.

6.4. System administrators are responsible for administering user account authentication and account management.

6.5. IT Services, in cooperation with departmental system managers, administrators and users, is responsible for providing information security training.

6.6. The Chief Administrative Officer and Associate Vice-President, Information Technology are responsible for monitoring and enforcing this policy.

7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure and it adheres to the principles outlined in the College’s commitment to accessibility as demonstrated by the Accessibility Plan (ADMIN-203).

8. Non-compliance implications

Non-compliance could affect the College's ability to conduct business, respond to requests for information, be transparent and accountable, and ensure confidentiality and privacy of personal information. This would be a risk to the College both financially and to its reputation in the community.

Failure to comply with this policy could result in loss of access to Durham College information technology services and equipment, disciplinary action up to and including suspension or termination of an employee, and/or legal action that could result in criminal or civil proceedings.

9. Communications plan

- A message will be posted on ICE alerting employees when new or revised policies and procedures are added to ICE.
- A message will be posted on MyCampus alerting students when new or revised policies and procedures are added.

10. Related forms, legislation or external resources

- Freedom of Information and Protection of Privacy Act (FIPPA)
- Personal Health Information Protection of Privacy Act (PHIPPA)