DOUGLAS COLLEGE

INFORMATION SECURITY POLICY

Policy Name: Information Security Policy	Responsible Owner: Vice President, Administrative Services and CFO	Created: 2013 Mar
Policy Number: A42	Approval Body: SMT	Last Reviewed/Revised: 2017 Jun
Category: Administrative	Replaces: A20.01.06	Next Review: 2020 Mar

TABLE OF CONTENTS

A. PURPOSE

Douglas College's information, network, and other IT services are shared resources that are critical to teaching, learning, research, College operations, and service delivery. The purpose of this policy is to:

- Protect the confidentiality, integrity, and availability of Douglas College information and associated information technology
- Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations
- Ensure the reliable operation of Douglas College's information technology so that all members of the Douglas College community have access to the information assets they require

B. SCOPE

This policy applies to all Douglas College information, computing, communications and networking resources connected to College facilities and to the users of these resources.

C. DEFINITIONS

1. **College Administrators:** Exempt management members with supervisory responsibility for a department, faculty or program.

2. **Information Owners:** Those responsible (often College Administrators) for the safety, accuracy, and access/use of information in their custody.

3. **System Owners:** Usually the responsible College Administrator in a department or program, and who make decisions about the selection, functions, and operation of a technology system in their area.

4. **Asset Custodians:** Each piece of technology equipment provided by the college must have an assigned asset custodian, who is responsible for the technology asset(s), and will manage location and function.

5. **IT Administrators:** Usually a member of CEIT for on-premises enterprise systems. For department specialty systems, the IT administrator may be a staff member in the department or a CEIT staff member. Hosted or cloud services must have an IT administrator identified, either within the college or at the host/cloud organization.

D. POLICY STATEMENTS

Douglas College will take appropriate measures to preserve the confidentiality, integrity, and availability of information, support information security within the organization, and to maintain a secure information technology (IT) environment. The College provides a safe and secure environment for the collection, storage, access and retrieval of information. Members of the College community are required to handle Douglas College information assets responsibly within their respective roles and in accordance with this policy.

1. The Douglas College Senior Management Team establishes and maintains an appropriate Information Security Framework and provides ongoing executive oversight of the framework, including periodic, independent reviews.

2. College Administrators are responsible for ensuring that employees and others under their supervision are aware of their information security responsibilities.

3. Teaching faculty are responsible for ensuring that students under their supervision are aware of their information security responsibilities, for all activities undertaken by said faculty.

4. Information Owners are responsible for classifying information in accordance with policies and guidelines. All information must have an assigned information owner.

5. System Owners are accountable for ensuring that systems are assessed for security requirements including those flowing from legislative and contractual obligations. System Owners are also accountable for ensuring that systems are designed, configured, implemented, operated, maintained, upgraded, and decommissioned consistent with the established security needs. All College systems must have an assigned System Owner. System Owners must ensure an IT Administrator and asset custodian are assigned to each asset comprising the system.

6. Asset Custodians, upon request, must be able to determine the location of technology assets under their custodianship and must ensure that assets transferred from their custodianship are clearly assigned to the next custodian. All physical assets such as information technology equipment must have an assigned custodian.

7. IT Administrators are responsible for configuring the security features of the assets under their administration in accordance with policy, guidelines, and other requirements. All assets with security settings that can be configured and/or changed must have an assigned IT Administrator.

8. CEIT, as the central provider of Information Technology, is responsible for:
   - Network management and operation including the establishment of network zones
   - Delegation of administration of a network zone only when appropriate controls are in place in the delegated organization
   - Maintaining a catalogue of core services including clearly articulated service level expectations
   - Continuity of core enterprise class IT infrastructure as part of the College's overall business continuity framework
   - Maintaining an inventory of college technology assets
   - Responding to and resolving real or suspected breaches of security including, but not limited to, unauthorized access, theft, system or network intrusions, willful damage, and fraud

9. All users are responsible for:
   - Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control
   - Promptly reporting all acts that may constitute real or suspected breaches of security including, but not limited to, unauthorized access, theft, system or network intrusions, willful damage, and fraud. Reporting must include direct supervisor and CEIT
   - Looking after any physical device (phones, computers, laptops, etc.) and access articles (keys, ID cards, system IDs, passwords, etc.) assigned to them for the purposes of performing their job duties, taking courses, conducting research, or otherwise participating within the College
   - Respecting the classification of information as established by the Information Owner
   - Complying with all the security requirements defined in this document and all supporting procedures, rules, and guidelines

E. PROCEDURES

Internal Guidelines

- Information Security Guidelines and Responsibilities
- Mobile Device Security Guideline
- Incident Response Guidelines and Responsibilities

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administration Policies Page

- Compliance with the Freedom of Information and Protection of Privacy Act
- College Use of Copyrighted Works
- Records Management and Retention Policy
- Acceptable Use of Computing and Information Technology Policy

G. RELATED ACTS AND REGULATIONS

- *College and Institute Act* (R.S.B.C. 1996 c. 52)
- *Freedom of Information and Protection of Privacy Act* (R.S.B.C. 1996 c. 165)
- *Criminal Code (R.S.C., 1985, c. C-46)*

- *Copyright Act (R.S.C., 1985, c. C-42)*

H. RELATED COLLECTIVE AGREEMENT CLAUSES

N/A