DOUGLAS COLLEGE

INFORMATION SECURITY POLICY

Policy Name: Information Security Policy	Responsible Owner: Associate Vice President, Technology and CIO	Created: 2013 Mar
Policy Number: A42	Approval Body: SMT	Last Reviewed/Revised: 2020 Mar
Category: Administration	Replaces: N/A	Next Review: 2025 Feb

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 (IT);
- Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations; and
- Ensure the reliable operation of Douglas College's IT so that all members of the Douglas College Community have access to the information assets they require.

B. SCOPE

This policy applies to all members of the College Community and governs their relationship with Douglas College information, computing, communications and networking resources connected to College facilities.

C. DEFINITIONS

College Administrators: Exempt management members with supervisory responsibility for a department or Faculty.

College Community: Includes all employees, students, users, contractors, suppliers, guests and any other person participating in any College-related activity or attending an event on College premises.

Confidential Data: Data classified as Level 3 (Highly Sensitive) or Level 4 (Personal and Regulated). Please see point 1 in Policy Statement for definitions of data classification levels.

Data Administrators: Persons responsible for granting appropriate access to users.

Data Custodians/System Administrators: Individuals responsible for properly storing, protecting, enabling use, and backing up of data and systems. Usually a member of CEIT for on-premises enterprise systems and a vendor for a cloud-hosted solution; may be a combination of CEIT staff and a vendor.

Data/System Users: Persons granted access to institutional data and/or systems in order to perform assigned duties or fulfil assigned roles or functions within an organization.

Data Trustee: Data Accountability Owner; an institutional officer with accountability for, and therefore authority over standards, guidelines and procedures regarding business definitions of data and the access and usage of that data within their authority.

Information Security Framework: An information security framework is a series of documented, agreed and understood policies, procedures, and processes that define how information is managed. Top information security frameworks include ISO 27001, NIST Framework for Improving Critical Infrastructure Security, CIS Critical Security Controls, and PCI DSS.

Least Privilege Principle: The principle that individuals (and systems) are granted only those privileges that they need to perform their work tasks and job functions. Privilege includes the ability to perform an action, such as accessing information directly within a system.

Need-to-Know Principle: The principle that individuals (and systems) are provided with only that information they need to know for their work tasks and job functions and at the time they need to know it. While some employees may need to be provided with certain information stored within a system, this need does not mean that they need to be able to access that information within that system by themselves.

System Owner: An individual with responsibility to ensure that data processed on a system remain secure. It may be a College Administrator within CEIT or a business area. Hosted or cloud services must have a College System Owner identified.

D. POLICY STATEMENTS

Douglas College will take appropriate measures to preserve the confidentiality, integrity and availability of information; to support information security within the organization; and to maintain a secure 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.

Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Students in violation of this policy may be subject to disciplinary action under Standards of Student Conduct Policy.

1. The following data classification levels are defined for College data and information:

    a. Level 1 – Public
    Data that is or can be publicly released without causing any harm to the College.

    b. Level 2 – Internal
    Data that if released may cause minor harm or embarrassment to the College.

    c. Level 3 – Highly Sensitive
    Data that if compromised can cause considerable harm or embarrassment to the College.

    d. Level 4 – Personal and Regulated
    Data that if compromised could result in long-term harm or reputational risk to the College and/or to individuals, such as breach reporting, negative press, lawsuits against the College, considerable loss of revenue.

    (See Data Classification Standard for more information.)

2. Access to data and systems should be granted based on "Need to Know" and/or "Least Privilege" principles. Data Trustees and System Owners need to ensure that these principles are followed.

    If individuals need to access specific information only occasionally, Data Trustees should consider ensuring that the information is provided only when needed, in order to reduce the College's exposure in case an account is compromised.

3. Data/System Users must not access any information they do not need to perform their immediate business responsibilities, regardless of whether this information is accessible to them.

Roles and Responsibilities

1. The Douglas College Senior Management Team (SMT) has ultimate responsibility for Information Security: SMT 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 and follow their information security responsibilities.

3. Teaching faculty are responsible for ensuring that their students are aware of their information security responsibilities for all College-related activities.

4. Data Trustees are accountable for ensuring classification of information in accordance with this policy and related standards, guidelines, and procedures. All types of College information must have an assigned Data Trustee, and each set of data must have only one Data Trustee, although Data Trustees may appoint Proxies as appropriate.

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 standards. All College systems must have an assigned System Owner.

6. System Owners are responsible for ensuring that all systems they are accountable for have an assigned System/Data Custodian(s) and that the custodianship is transferred properly when appropriate.

7. Data/System Custodians (also known as System Administrators) are responsible for configuring the security features of the assets under their administration in accordance with relevant policies, standards, and guidelines. All assets with security settings that can be configured and/or changed must have an assigned System Administrator.

8. As the central provider of IT, CEIT 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 or fraud

9. All users are responsible for:

    - Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control
    - Secure storage, archival, and disposal of confidential documents in paper and portable media format in their custody
    - 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 Data Trustee
    - Classifying information created by them as per rules established by a Data Trustee

- Complying with all security requirements defined in this document and all supporting standards. Guidelines should be followed whenever possible. Procedures should be followed, when available, to help improve compliance with policies, standards, and guidelines.

E. PROCEDURES

Violations of this policy may constitute a Reportable Activity as defined in the College's *Protected Disclosure (Whistleblower) Policy* and should be reported in accordance with the procedures found in that policy.

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administration Policies

- *Acceptable Use of Computer and Information Technology Policy*
- *College Use of Copyrighted Works Policy*
- *Compliance with the Freedom of Information and Protection of Privacy Act Policy*
- *Protected Disclosure (Whistleblower) Policy*
- *Records and Information Management Policy*

Applicable Standards (available on DC Connect)

- Data Classification Standard
- Information Security Standards and Guidelines
- IT Security Incident Response Standard

G. RELATED ACTS AND REGULATIONS

- *College and Institute Act* (R.S.B.C. 1996 c. 52)
- *Copyright Act (R.S.C., 1985, c. C-42)*
- *Criminal Code (R.S.C., 1985, c. C-46)*
- *Freedom of Information and Protection of Privacy Act* (R.S.B.C. 1996 c. 165)

H. RELATED COLLECTIVE AGREEMENTS

N/A