DOUGLASCOLLEGE

INFORMATION SECURITY POLICY

Policy Name: Information Security	**Responsible Owner:** Associate Vice President, Technology and CIO	**Created:** 2013 Mar
Policy Number: A42	**Approval Body:** SMT	**Last Reviewed/Revised:** 2024 Jun
Category: Administration	**Replaces:** N/A	**Next Review:** 2027 Jun

TABLE OF CONTENTS

A. PURPOSE

Douglas College's information, network, and other information technology (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 information and associated IT at Douglas College (the College);
- Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations; and
- Ensure the reliable operation of the College's IT so that all members of the 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, network and devices used to connect to College facilities.

C. DEFINITIONS

College Community: All College employees, students and Board members, and any other person contractually obligated to comply with College policy; for the purposes of this policy, includes all College facility users, contractors, suppliers, guests and other persons participating in any College-related activity or attending an event sponsored, led or organized by the College (online or in person).

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

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; a Responsible Administrator with accountability for and authority over standards, guidelines and procedures regarding business definitions of data and the access to and use of that data under their authority.

Information Security Framework: A series of documented, agreed and understood policies, procedures, and processes that define how information is managed, such as International Organization for Standardization (ISO) 27001, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Security, the Centre for Internet Security Critical Security Controls and the Payment Card Industry Data Security Standard.

Least Privilege Principle: The principle that individuals (and systems) are to be granted only those privileges needed to perform their work tasks and job functions, including 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 to be provided with only that information needed to do 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, they may not need to access that information by themselves.

Responsible Administrator: An executive of the College or an administrator responsible for the operations of a College department, Faculty or service area (e.g., Dean, Director, Chief Information Officer, Registrar).

System Business Owner: An individual with overall responsibility for the system; works with the IT Security team, product vendor and/or Privacy Officer (as applicable); also known as System Owner.

System Technical Owners: Individuals responsible for properly storing, protecting, enabling the use and backing up of data and systems; usually a member of Information Technology (IT) Services for on-premises enterprise systems or a vendor for a cloud-hosted solution, but may involve both IT Services staff and a vendor; also known as custodians.

D. POLICY STATEMENTS

1. Douglas College provides a safe and secure environment for the collection, storage, access to and retrieval of information. The College will take appropriate measures to

    a. Preserve the confidentiality, integrity and availability of information;
    b. Support information security within the organization; and
    c. Maintain a secure information technology (IT) environment.

2. Members of the College Community are required to handle College information assets responsibly within their respective roles and in accordance with this policy.

    a. Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
    b. Students found to have violated this policy may be subject to disciplinary action under the appropriate policy governing student conduct.

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

    a. Level 1 – Public
    Data that are or can be publicly released without causing any harm to the College or a person.
    b. Level 2 – Internal (or Sensitive)
    Data that if released may cause minor harm or embarrassment to the College or a person.
    c. Level 3 – Highly Sensitive
    Confidential data that if compromised can cause considerable harm or embarrassment to the College or a person.

    (*See* Data Classification Standard *for more information.*)

4. All College systems must have an assigned System Business Owner, and all assets with security settings that can be configured and/or changed must have an assigned System Technical Owner.

5. Access to data and systems should be granted based on Need to Know and/or Least Privilege Principle.

6. 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.

7. Individuals may not authorize access to systems and data for themselves; IT Services requires authorization from an employee's Responsible Administrator or Data Trustee.

Roles and Responsibilities

8. 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 it, including periodic, independent reviews.

9. Responsible Administrators are responsible for ensuring that employees and others under their supervision are aware of and follow their information security responsibilities.

10. Data Trustees are accountable for ensuring

    a. the classification of information in accordance with this policy and related standards, guidelines, and procedures; and
    b. that the principles of Need to Know and Least Privilege are followed

    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.

11. System Business Owners are accountable for ensuring

    a. that the principles of Need to Know and Least Privilege are followed; and
    b. that all systems they are accountable for
        i. are assessed for security requirements, including those flowing from legislative and contractual obligations;
        ii. are designed, configured, implemented, operated, maintained, upgraded and decommissioned consistent with established security standards; and
        iii. have an assigned System Technical Owner, with the custodianship transferred properly when appropriate.

12. System Technical Owners are responsible for configuring the security features of the assets under their administration in accordance with relevant policies, standards, and guidelines.

13. As the central provider of IT, IT Services is responsible for the following:

    a. Managing and operating the network, including the establishment of network zones;
    b. Delegating administration of a network zone only when appropriate controls are in place in the delegated organization;
    c. Maintaining a catalogue of core services, including clearly articulated service level expectations;
    d. Ensuring continuity of core enterprise-class IT infrastructure as part of the College's overall business continuity framework;
    e. Maintaining an inventory of College technology assets; and
    f. 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.

14. All users are responsible for:

    a. Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control;
    b. Ensuring the secure storage, archiving and disposal of highly sensitive documents in their custody, in either paper or portable media format;
    c. Looking after any physical device (e.g., phones, computers, laptops) and access articles (e.g., keys, ID cards, system IDs, passwords) assigned to them for the purposes of performing their job duties, taking courses, conducting research, or otherwise participating within the College;
    d. Respecting the classification of information as established by a Data Trustee;
    e. Classifying information created by them as per rules established by a Data Trustee;
    f. Complying with all security requirements defined in this document and all supporting standards, guidelines and procedures;
    g. Ensuring that confidential information is never sent to a shared printer without an authorized user ensuring that it is immediately retrieved; and
    h. Ensuring that areas, systems and devices are not left unattended or unprotected if this may result in someone gaining unauthorized access to confidential or internal information.

E. PROCEDURES

Behaviours that might constitute an Information Security breach should be reported immediately to the Information Technology (IT) Services Service Desk.

Responding to Alleged Breaches of Information Security

1. Upon receipt of a report of a possible breach of Information Security, IT Services staff will escalate the report to the IT Security team for initial review.

2. If IT Security determines that the report has substance, the IT Security team will immediately

    a. Suspend the access to College networks and information systems of all person(s) suspected to have breached the College's information security; and
    b. Contact the relevant Responsible Administrator(s) and SSRM, who will form a Cyber Threat Response Team (CTRT) to investigate the breach of information security. The CTRT will bring in additional personnel as required (e.g., the College's Privacy Officer, law enforcement).

3. IT Services will not re-instate access to College networks or information systems without prior authorization from the CTRT.

4. Violations of the *Information Security Policy* may constitute breaches of other College policies. CTRT investigations will be conducted consistent with applicable policy/policies. Violations of this policy by a Student may constitute misconduct as defined in the College's *Student Non-academic Misconduct Policy* and will be investigated consistent with that policy.

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administration Policies

- *Acceptable Use of Computer and Information Technology*
- *College Use of Copyrighted Works*
- *Privacy*
- *Public Interest Disclosure (Whistleblower)*
- *Records and Information Management*
- *Student Non-academic Misconduct*

Applicable Standards (available on DC Connect – for internal users only)

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

G. RELATED ACTS AND REGULATIONS

- *College and Institute Act* [RSBC 1996], c. 52
- *Copyright Act* [RSC 1985], c. C-42
- *Criminal Code* [RSC 1985], c. C-46
- *Freedom of Information and Protection of Privacy Act* [RSBC 1996], c. 165
- *Public Interest Disclosure Act* [SBC 2018], c. 22

H. RELATED COLLECTIVE AGREEMENTS

N/A