Dawson COLLEGE

**No. IST-07**

| **Title:** | **Identity and Access Management Policy** |
|---|---|

**CLASSIFICATION:** Information Systems & Technology
**FIRST ADOPTED:** 9 June 2025
**AMENDED:**

## 1 Preamble

The goal of this policy is to protect information by ensuring that only authorized users, according to their duties and responsibilities, can access it. It outlines the requirements to verify user identities, grant access, and keep systems safe from unauthorized use.

## 2 Scope

This policy applies to all students, employees and any other individuals who are granted access to information assets managed by Dawson College.

## 3 Legal and Administrative framework

- The Act respecting the governance and management of the information resources of public bodies and government enterprises (CQLR, chapter G-1.03) defines the governance and regulatory framework for public bodies.
- The Password policy (IST-03) defines the principles and key requirements for password protection.
- The Accounts policy (IST-04) defines the types of accounts and specific requirements related to their creation and use.
- The Authority register (IST-06) defines the information assets and their owner.

## 4 Definitions

- **Asset owner**. The individual responsible for the management of an information asset.
- **Generic account**. An account that is not tied to a specific individual.
- **Information asset**. A collection of information accessed through a system or online service.
- **Least privilege principle.** The information security concept that ensures users are given the minimum levels of access or permissions needed to perform their job functions.
- **Shared account**. A generic account designed to be shared among users.
- **User**. An individual who is granted access to information assets: a student, an employee or an external person.

## 5 Account Creation and Management

Requirements for the creation of accounts are outlined in the Accounts policy.

- Only one individual can be assigned to an account, with the exceptions of generic and shared accounts, which can be created under the provisions outlined by the Accounts policy.
- All accounts must have a unique reference to the user, with the exception of generic and shared accounts. For students, the reference is a student number, for employees, an employee number. For external users, the contact information is required.
- Employees who have different roles may have more than one account, subject to the least privilege principle.

## 6 Authentication and Password Management

Authentication is the process of verifying the identity of a user. A password is the primary authentication factor, but multi-factor authentication (MFA) may be required, or additional factors for certain roles or sensitive information.

Password requirements, including complexity, length and aging, are outlined in the Password policy.

## 7 Access Control

Access to systems and data are granted according to the following principles:

- Role-based access control. Access is based on the user's role within the College.
- Least privilege. Under this principle, some employees will have multiple accounts to separate their duties. For example, a user with access to sensitive financial data might have a regular user account for day-to-day activities and a separate account with higher privileges for accessing financial systems.
- Segregation of duties. This principle ensures that no one user has complete control over processes and information. For example, the person approving access is not the same person assigning roles and permissions.

Granting exceptional access privileges must be authorized by the reporting manager and by the asset owner.

Periodical reviews of user access rights are conducted to ensure compliance with this policy.

## 8 Transfer, Leaves and Departures

Accounts are deactivated when a user leaves the college or no longer requires access.

The departure or transfer of a user, or any other change to their tasks and functions, leads to a review of their access privileges.

Data associated with deactivated accounts are retained or deleted in accordance with the College Retention Schedule.

## 9 Roles and Responsibilities

Users have a responsibility to report to IT Support any suspicious activity, incident or breach involving their account.

### 9.1 Asset Owners

- Ensure the security and integrity of the information assets they manage.
- Define the process to create accounts or grant access.
- Define the access privileges associated to a role.
- Approve the creation of high privilege accounts.
- Approve exceptional access requests.
- Conduct access privilege reviews to ensure compliance with this policy.

### 9.2 Managers

- Conduct periodic reviews of the access privilege granted to users who report to them and to external users under their purview.
- Conduct a review of the access privileges granted to users leaving or changing roles in their unit, and ensure their access is revoked or updated, as necessary. In cases where an employee moves to another unit and temporarily retains some access privileges from their previous role, the previous and the new reporting manager should consult each other.

## 10 Policy Application

The Director of Information Systems and Technology is responsible for the review and the application of this policy.