N° IST-07

Titre :	**Politique de gestion des identités et des accès**

CLASSIFICATION : Technologies & Systèmes d'Information
PREMIÈRE ADOPTION : 9 Juin 2025
MODIFIÉ :

Cette politique a été adoptée en anglais. En cas de divergence la version anglaise prévaut sur la version française.

1 Préambule

L'objectif de cette politique est de protéger les informations en veillant à ce que seuls les utilisateurs autorisés, conformément à leurs fonctions et responsabilités, puissent y accéder. Elle décrit les exigences relatives à la vérification de l'identité des utilisateurs, à l'octroi de l'accès et à la protection des systèmes contre toute utilisation non autorisée.

2 Champ d'application

Cette politique s'applique à toute personne étudiante, employée ou autrement autorisée à accéder aux informations gérées par le Collège Dawson.

3 Cadre juridique et administratif

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03) définit le cadre de gouvernance et de réglementation des organismes publics.
- La politique relative aux mots de passe (IST-03) définit les principes et les principales exigences en matière de protection par mot de passe.
- La politique des comptes (IST-04) définit les types de comptes et les exigences spécifiques liées à leur création et à leur utilisation.
- Le registre d'autorité (IST-06) définit les actifs informationnels et leur propriétaire.

4 Définitions

- **Propriétaire du bien**. Personne responsable de la gestion d'un actif informationnel.
- **Compte générique**. Un compte qui n'est pas lié à une personne spécifique.
- **Actif informationnel**. Ensemble d'informations auxquelles on accède par l'intermédiaire d'un système ou d'un service en ligne.
- **Principe du moindre privilège.** Concept de sécurité de l'information qui garantit que les utilisateurs disposent des niveaux d'accès ou des autorisations minimales nécessaires pour exercer leurs fonctions.

- **Compte partagé**. Compte générique conçu pour être partagé entre les utilisateurs.
- **Utilisateur**. Une personne à qui l'on accorde l'accès aux ressources d'information : un étudiant, un employé ou une personne externe.

5 Création et gestion de comptes

Les exigences relatives à la création de comptes sont décrites dans la politique en matière de comptes.

- Une seule personne peut être affectée à un compte, à l'exception des comptes génériques et partagés, qui peuvent être créés conformément aux dispositions de la politique des comptes.
- Tous les comptes doivent avoir une référence unique à l'utilisateur, à l'exception des comptes génériques et partagés. Pour les étudiants, la référence est un numéro d'étudiant, pour les employés, un numéro d'employé. Pour les utilisateurs externes, les informations de contact sont obligatoires.
- Les employés qui ont des rôles différents peuvent avoir plus d'un compte, sous réserve du principe du moindre privilège.

6 Authentification et gestion des mots de passe

L'authentification est le processus de vérification de l'identité d'un utilisateur. Un mot de passe est le principal facteur d'authentification, mais une authentification multifactorielle (MFA) peut être requise, ou des facteurs supplémentaires pour certains rôles ou informations sensibles.

Les exigences en matière de mot de passe, y compris la complexité, la longueur et le vieillissement, sont décrites dans la politique relative aux mots de passe.

7 Contrôle d'accès

L'accès aux systèmes et aux données est accordé selon les principes suivants :

- Contrôle d'accès basé sur le rôle. L'accès est basé sur le rôle de l'utilisateur au sein du Collège.
- Le moindre privilège. En vertu de ce principe, certains employés disposeront de plusieurs comptes afin de séparer leurs tâches. Par exemple, un utilisateur ayant accès à des données financières sensibles peut disposer d'un compte d'utilisateur normal pour ses activités quotidiennes et d'un compte distinct doté de privilèges plus élevés pour accéder aux systèmes financiers.
- Séparation des tâches. Ce principe garantit qu'aucun utilisateur n'a le contrôle total des processus et des informations. Par exemple, la personne qui approuve l'accès n'est pas la même que celle qui attribue les rôles et les autorisations.

L'octroi de privilèges d'accès exceptionnels doit être autorisé par le supérieur hiérarchique et par le propriétaire du bien.

Des examens périodiques des droits d'accès des utilisateurs sont effectués pour garantir le respect de cette politique.

8 Transferts, congés et départs

Les comptes sont désactivés lorsque l'utilisateur quitte le collège ou n'a plus besoin d'accès.

Le départ ou le transfert d'un utilisateur, ou toute autre modification de ses tâches et fonctions, entraîne une révision de ses privilèges d'accès.

Les données associées aux comptes désactivés sont conservées ou supprimées conformément au calendrier de conservation du Collège.

9 Rôles et responsabilités

Les utilisateurs ont la responsabilité de signaler à l'assistance informatique toute activité suspecte, tout incident ou toute infraction concernant leur compte.

9.1 Propriétaires d'actifs

- Garantir la sécurité et l'intégrité des informations qu'ils gèrent.
- Définissez le processus de création de comptes ou d'octroi d'accès.
- Définir les privilèges d'accès associés à un rôle.
- Approuver la création de comptes à privilèges élevés.
- Approuver les demandes d'accès exceptionnel.
- Procéder à l'examen des privilèges d'accès afin de garantir le respect de la présente politique.

9.2 Gestionnaires

- Procéder à des examens périodiques des privilèges d'accès accordés aux utilisateurs qui leur rendent compte et aux utilisateurs externes qui relèvent de leur compétence.
- Passez en revue les privilèges d'accès accordés aux utilisateurs qui quittent ou changent de rôle dans leur unité et veillez à ce que leur accès soit révoqué ou mis à jour, le cas échéant. Lorsqu'un employé est muté dans une autre unité et qu'il conserve temporairement certains privilèges d'accès liés à son rôle précédent, l'ancien et le nouveau responsable hiérarchique doivent se consulter mutuellement.

10 Application de la politique

Le directeur des Technologies et Systèmes d'Information est responsable de la révision et de l'application de cette politique.