CollègeAhuntsic

RECUEIL DES
RÈGLES DE GESTION

DIRECTIVE DE LA GESTION DES IDENTITÉS ET DES ACCÈS

(D-26)

RECUEIL DES RÈGLES DE GESTION

DIRECTIVE DE LA GESTION DES ACCÈS ET DES IDENTITÉS

(D-26)

Adoptée par le Comité de direction le 31 janvier 2023

Table des matières

PRÉAMBULE **1**

ARTICLE 1.00 — DÉFINITIONS **1**

ARTICLE 2.00 — OBJECTIFS **4**

ARTICLE 3.00 — CADRE JURIDIQUE **4**

ARTICLE 4.00 — CHAMPS D'APPLICATION **4**

ARTICLE 5.00 — SÉPARATION DES TÂCHES **4**

ARTICLE 6.00 — COMPTES À PRIVILÈGES SPÉCIAUX **5**

ARTICLE 7.00 — RÔLES ET RESPONSABILITÉS **5**

ARTICLE 8.00 — RESPONSABLE DE LA DIRECTIVE **8**

ARTICLE 9.00 — ENTRÉE EN VIGUEUR ET RÉVISION **8**

DIRECTIVE DE LA GESTION DES ACCÈS ET DES IDENTITÉS (D-26)

PRÉAMBULE

Le Collège Ahuntsic reconnait l'importance de donner accès à ses actifs informationnels, dont ses équipements et ses ressources informatiques et de télécommunication, aux membres de la communauté. La présente directive vise à concilier les besoins communs et individuels, puisque si l'on cherche à protéger les actifs informationnels du Collège, c'est pour les rendre disponibles à l'utilisation. Ainsi, la Directive établit les conditions relatives à l'utilisation sécuritaire, par les personnes recourant aux services du Collège, des équipements, des systèmes, des logiciels, du réseau, des documents analogiques de même que des données contenues ou véhiculées. Le but de cette démarche est de réduire les risques liés à la sécurité de l'information et, ainsi, de protéger les renseignements critiques du Collège, les renseignements personnels des membres de la communauté ainsi que la vie privée de chaque personne.

La gestion des identités et des accès est basée sur les principes suivants : besoin de savoir et besoin d'utiliser. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des ressources. Cette gestion comprend un aspect administratif, couvert par des politiques, directives et procédure, ainsi que des aspects logiques et physiques, basés sur l'attribution explicite de toute autorisation, le moindre privilège et la séparation des tâches.

La présente Directive définit certaines modalités opérationnelles découlant des principes directeurs de la *Politique de sécurité de l'information* (PO-33) et de la *Politique sur l'utilisation des technologies de l'information* (PO-27). Ces modalités guideront les personnes autorisées dans l'utilisation des actifs informationnels du Collège afin d'assurer la sécurité de l'information tout au long de son cycle de vie tout en renforçant l'efficacité et la transparence des opérations.

ARTICLE 1.00 — DÉFINITIONS

Dans cette Directive, les expressions et les termes suivants signifient :

a) **« Accès »** : Droit ou permission obtenus de consulter, de modifier ou de supprimer physiquement ou logiquement un actif informationnel.

b) **« Actif informationnel »** : Information numérique, document numérique ou analogique, système d'information, documentation, matériel informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitués par le Collège pour mener à bien sa mission, qu'ils soient détenus ou exploités par le Collège, par des prestataires de services ou par des tiers.

c) **« Authentification »** : Processus visant à vérifier une identité en la comparant aux valeurs enregistrées dans un annuaire d'identités. L'authentification permet de s'assurer que les personnes utilisatrices sont bien qui elles prétendent être.

d) **« Autorisation »** : Processus permettant de déterminer les types d'activités permises. Attribution à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

e) **« Confidentialité »** : Propriété d'informations ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées.

f) **« Comptes à privilèges spéciaux »** : Comptes administrateurs, intégrés ou de services qui permettent des accès élevés.

g) **« Disponibilité »** : Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

h) **« Document analogique »** : Document sur papier, film ou microformes (bobine, microfiche, microfilm ou carte à fenêtre).

i) **« Gestion des accès »** : Ensemble des contrôles logiques et physiques qui permettent, lorsque des personnes ou des entités tentent d'accéder à un actif informationnel, de les identifier, de les authentifier et de leur en autoriser l'accès. Ces contrôles visent à protéger les données au repos, en transit et en utilisation des risques de fuites, de corruption, d'attaques et de négligences humaines. Un bon système de gestion des accès doit également prévenir la non-répudiation.

j) **« Gestion des identités »** : Ensemble des processus informatiques qui gèrent la création, la modification, la résiliation, la validation, l'approbation, la diffusion et la communication d'une identité pour une personne ou une machine accompagnée de leurs processus de contrôle, qu'ils soient manuels ou automatiques.

k) **« Identifiant »** : Information fournie par une personne ou une entité pour décliner son identité afin d'accéder à un réseau, à un système, à une application ou à un lieu physique. Il peut s'agir, par exemple, d'une carte bancaire, d'un nom d'utilisateur, d'une adresse de courrier électronique ou d'un numéro de compte.

l) **« Identité »** : Séquence ou ensemble unique de caractéristiques permettant d'identifier un individu ou un compte de façon univoque.

m) **« Incident »** : Évènement qui porte atteinte, ou qui est susceptible de porter atteinte, à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

n) **« Information »** : Renseignement consigné sur tout support pour être conservé, traité ou communiqué.

o) **« Information institutionnelle protégée »** : Information protégée par la loi ou dont l'usage est régi par contrat, par une politique, par un règlement ou une directive du Collège de par sa nature confidentielle et/ou stratégique. Par exemple, tout document financier ou critique aux opérations du Collège.

p) **« Intégrité »** : Propriété d'une information intacte, entière, qui n'a pas été altérée, volontairement ou accidentellement, lors de son traitement ou de sa transmission.

q) **« Non-répudiation »** : Impossibilité pour une partie de nier avoir participé en totalité ou en partie à un échange, du fait de l'existence de contrôles d'authentification, d'accusés de réception et de pistes d'audit efficaces.

r) **« Permission »** : Autorisation donnée à une personne dument authentifiée d'accéder à des données et de procéder à des opérations informatiques en fonction des droits d'accès qui lui ont été préalablement attribués.

s) **« Pilote de système »** : Utilisateur ou utilisatrice du système, qui se charge des configurations avancées dans le système et qui a l'autorisation d'exécuter des fonctions liées à la sécurité. Les pilotes de système sont aussi responsables de faire des essais d'utilisation avant les mises en production du système.

t) **« Propriétaire de système » :** Dans l'organisation, personne responsable de l'acquisition, du développement, de l'intégration, de la modification, de l'exploitation, de la maintenance et de l'élimination d'un système.

u) **« Registre de gestion des identités et des accès »** : Système de stockage des données contenant toutes les données actuelles et historiques relatives au système de gestion des identités et des

accès.

v) **« Renseignement personnel »** : Renseignement qui, dans un document, concerne une personne physique et permet de l'identifier. Par exemple, et non limitativement, le nom, l'adresse, le numéro de téléphone personnel, le statut de fréquentation, le code permanent, le numéro d'employé, la date de naissance, les informations médicales et les numéros de cartes de paiement.

w) **« Ressource »** : Élément du système de gestion des identités et des accès (GIA) qui peut être demandé par une personne. Il peut s'agir d'une application, d'un composant de l'infrastructure technologique (par exemple, un système), d'un accès ou d'une habilitation spécifique (par exemple, un groupe ou un profil).

x) **« Risque de sécurité de l'information »** : Degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bienêtre des personnes, sur la protection de leurs renseignements personnels, le respect de leur vie privée, ou sur l'image du Collège.

y) **« Rôle » :** Regroupement de fonctions similaires ; un rôle, déterminé par une autorité centrale, associe à un sujet des autorisations d'accès sur un ensemble d'objets.

z) **« S'assurer » :** Responsabilité de faire, déléguer ou sous-traiter une action.

aa) **« Sécurité de l'information »** : Ensemble de contrôles physiques, informatiques et administratifs, et de mesures d'urgence mises en place dans une organisation, en vue d'assurer la protection de l'ensemble de ses actifs informationnels. Plus particulièrement, la sécurité informationnelle assure l'intégrité, la confidentialité, l'authenticité, l'imputabilité, la non-répudiation et la fiabilité des actifs informationnels.

bb) **« Séparation des tâches »** : Mécanisme de contrôle qui consiste à désigne**r** plus d'une personne pour accomplir une tâche relative à l'autorisation et à l'enregistrement des opérations ou à la garde des actifs afin de réduire les possibilités qu'une même personne puisse commettre et dissimuler des erreurs ou des fraudes dans le cadre normal de l'exercice de ses fonctions.

cc) **« Sous-réseau »** : Segment d'un réseau qui peut être physiquement autonome et constituer une unité.

dd) **« Super utilisateur » :** Personne de référence pour ceux et celles qui ont des questions relatives à l'utilisation d'actifs informationnels du Collège.

ee) **« Système d'information »** : Système constitué des technologies de l'information, des procédures, ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.

ff) **« Technologie de l'information »** : Ensemble du matériel informatique, logiciels, réseau de télécommunication, services technologiques ainsi que les moyens et les méthodes de Sécurité de l'information utilisés pour la collecte, le stockage, le traitement, la transmission, la reproduction, la protection et l'élimination de l'information numérique.

gg) **« Utilisateur ou utilisatrice »** : Toute personne physique ou morale utilisant ou ayant accès aux actifs informationnels du Collège. Entrent notamment dans cette catégorie le personnel enseignant, le personnel professionnel, le personnel de soutien, le personnel-cadre, les étudiantes et étudiants, les organisations syndicales ou associatives qui les représentent, les locataires de la résidence étudiante, les personnes retraitées du Collège, ainsi que les prestataires de services externes.

ARTICLE 2.00 — OBJECTIFS

La présente Directive vise les objectifs suivants :

2.01 Mettre en place un processus garantissant que toutes les identités et tous les accès soient initiés, modifiés, suivis, enregistrés et résiliés à l'aide d'une ressource informatique ou par les personnes désignées par le Collège. Bien que les accès couverts par la *Directive sur l'utilisation de l'infonuagique* (D-24) ne soient pas concernés, leur gestion ne doit pas contrevenir à la présente Directive ;

2.02 Identifier les personnes responsables de la gestion des identités et des accès ;

2.03 Mettre en place un processus qui permet d'identifier, d'authentifier et d'autoriser tous les accès aux actifs informationnels du Collège et d'en assurer la non-répudiation en prenant en considération les limitations des systèmes de gestion ;

2.04 Réduire les risques relatifs à la sécurité de l'information en établissant les contrôles adéquats en gestion des identités et des accès.

ARTICLE 3.00 — CADRE JURIDIQUE

La présente Politique est soumise, notamment, aux dispositions de :

a) La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) *;*

b) La *Loi concernant le cadre juridique des technologies et l'information* (L.R.Q., c. C-1.1) ;

c) La *Loi sur la protection des renseignements personnels et les documents électroniques* (L.P.R.P.D.E. L.C. 2000, ch.5) ;

d) La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.G.G.R.I.) (L.R.Q., c. G-1.03) ;

e) Le *Code civil du Québec* ;

f) La *Charte des droits et libertés de la personne* (L.R.Q., c. C-12) ;

g) Les conventions collectives en vigueur au Collège.

De plus, elle complète les règlements et politiques suivants du Collège :

h) La *Politique de gestion intégrée des documents* (PO-24) ;

i) La *Politique sur l'utilisation des technologies de l'information* (PO-27) ;

j) *La Politique de sécurité de l'information* (PO-33) ;

k) La *Directive sur l'utilisation de l'infonuagique* (D-24).

ARTICLE 4.00 — CHAMPS D'APPLICATION

4.01 La présente directive s'applique à tous les actifs informationnels du Collège, indépendamment de l'endroit où ils sont utilisés, et s'adresse à toutes les personnes qui y ont accès.

ARTICLE 5.00 — SÉPARATION DES TÂCHES

5.01 Le principe de séparation des tâches permet d'éviter qu'une seule et même personne effectue l'ensemble des tâches d'un processus. Cette bonne pratique de sécurité informationnelle implique la segmentation des tâches, que ce soit au sein d'une même unité administrative ou entre plusieurs unités administratives, et diminue ainsi les risques d'usurpation d'identité et de fraude. Cependant, lorsque c'est nécessaire, le Collège peut se doter de pratiques différentes pour assurer le bon fonctionnement de ses activités.

ARTICLE 6.00 — COMPTES À PRIVILÈGES SPÉCIAUX

6.01 Les comptes à privilèges spéciaux doivent faire l'objet de mesures particulières, compte tenu des droits plus élevés qu'ils ont sur les actifs informationnels qu'ils contrôlent ; en effet, ces droits ont un impact sur l'intégrité des données.

L'un des principaux risques relatifs à la sécurité est l'utilisation inappropriée et globale des comptes à privilèges spéciaux combinée à une erreur humaine. Ce risque est mitigé lorsque l'on utilise le principe du moindre privilège. Il est recommandé de :

a) Ne les utiliser que lorsque requis et nécessaire.

b) En limiter l'accès à la Direction des technologies de l'information (DTI) et aux pilotes de système ;

c) Activer l'authentification à multifacteurs lorsque c'est possible ;

d) Changer les informations de connexion périodiquement ;

e) Consigner l'utilisation (journaliser) ;

f) Activer la notification de connexion lorsque c'est possible ;

g) Garder un inventaire de leur utilisation ;

h) Réexaminer régulièrement les droits accordés, en fonction de leur pertinence et de leur nécessité d'utilisation ;

i) Procéder au retrait des accès lorsque la personne concernée quitte ses fonctions.

ARTICLE 7.00 — RÔLES ET RESPONSABILITÉS

7.01 - Utilisateurs/Utilisatrices

Les utilisateurs et utilisatrices ont la responsabilité de :

7.01.1 Utiliser uniquement les accès qui leur ont été accordés. En aucun cas, ces accès ne doivent être partagés. Chaque personne doit préserver la confidentialité de ses codes d'accès et est imputable de leur utilisation. L'usurpation ou la tentative d'usurpation d'identité d'une autre personne physique ou morale *est passible de sanction* ;

7.01.2 Rapporter un incident relatif à la sécurité à la Direction des technologies de l'information en cas d'accès à des actifs informationnels qui ne sont pas nécessaires à l'accomplissement de leur travail ;

7.01.3 Utiliser un mot de passe différent pour chaque système. Aucun mot de passe lié à un compte professionnel ne doit être utilisé sur des comptes personnels. De plus, le courriel du Collège ne doit pas servir d'identifiant à des systèmes ou applications non reliés au Collège ;

7.01.4 Attribuer des accès aux données critiques ou sensibles seulement lorsque cela est nécessaire, et ce, pour la plus courte période possible ;

7.01.5 S'assurer de protéger les informations institutionnelles protégées du Collège lors d'une absence, en appliquant la politique du bureau et de l'écran vides, ne laissant ainsi aucune information sans surveillance ;

7.01.6 Ne pas accéder à des locaux contenant des actifs informationnels sans l'autorisation explicite du service ou du département responsable ;

7.01.7 Protéger leurs clés et leurs cartes d'accès, qui ne doivent en aucun cas être partagées ; les personnes à qui elles sont confiées sont imputables de tout incident lié à leur utilisation ;

7.01.8 Prendre connaissance de la présente directive, des mesures disciplinaires et des sanctions prévues au Règlement relatif à la sécurité et à la protection des personnes et des biens (R-14) pouvant être appliquées lorsque des actifs informationnels du Collège ont été mis en danger par une infraction découlant d'un comportement imprudent ou malveillant;

7.01.9 Ne jamais laisser les collaborateurs internes ou prestataires de services externes seuls dans un endroit donnant un accès physique à de l'information sensible ou critique, telle qu'identifiée par la catégorisation de l'information ;

7.01.10 S'assurer que les codes d'accès, mots de passe et clés de chiffrement utilisés pour sécuriser un document numérique appartenant au Collège peuvent être communiqués à leur supérieur hiérarchique sur demande.

7.02 - Gestionnaire

Les gestionnaires, responsables d'un service ou d'une unité administrative, doivent :

7.02.1 Fournir la présente directive à leur personnel et aux tiers avec lesquels ils et elles collaborent afin que les exigences en matière de sécurité de l'information soient respectées dans tout processus et tout contrat sous leur responsabilité ;

7.02.2 S'assurer que les droits d'accès sont ajustés, c'est-à-dire accordés, modifiés ou retirés, lorsqu'une personne sous leur responsabilité obtient un poste, change de rôle, s'absente temporairement ou quitte ses fonctions ;

7.02.3 S'assurer que les droits d'accès fournis à des utilisateurs ou utilisatrices pour des projets spécifiques sont retirés à la fin du mandat :

a. Faire le suivi avec les pilotes qui ont accordé des accès à leur système pour qu'ils soient retirés ;

b. Faire le suivi avec la Direction des technologies de l'information pour que les accès aux partages et aux licences à accès limités soient retirés ;

c. Faire le suivi avec le Service de l'équipement pour que les clés et les cartes d'accès soient récupérées.

7.02.4 S'assurer que les prestataires de services externes ne soient jamais seuls dans un endroit donnant un accès physique à de l'information sensible ou critique, telle qu'identifiée par la catégorisation de l'information ;

7.02.5 Collaborer avec la Direction des technologies de l'information afin que les actifs informationnels dont elle a besoin soient correctement maintenus ;

7.02.6 Rapporter à la Direction des technologies de l'information tout problème lié à l'application de la présente directive.

7.03 - Pilote de système

Les pilotes de systèmes doivent :

7.03.1 Attribuer, modifier ou retirer les accès au système sous leur responsabilité. Toute personne n'a accès qu'aux informations et aux fonctionnalités dont elle a besoin pour effectuer ses tâches ;

7.03.2 Contrôler l'attribution et l'utilisation des comptes à privilèges spéciaux. Leur utilisation doit en effet être restreinte et validée. Ces comptes doivent être utilisés uniquement lorsque nécessaire ; le rôle lié à l'administration du système sera alors séparé de celui rattaché à l'utilisation quotidienne et deux comptes distincts seront attribués à une personne qui assume deux rôles différents sur la même plateforme ;

7.03.3 Revoir périodiquement les droits d'accès accordés aux systèmes sous sa responsabilité et en informer les propriétaires selon les règles du service ou du département ;

7.03.4 Mettre en place et utiliser un registre de gestion des identités et des accès.

7.04 - Direction des ressources humaines

La Direction des ressources humaines a la responsabilité de :

7.04.1 Communiquer aux pilotes des systèmes, les absences prolongées, les changements de fonctions et les départs afin que les accès puissent être modifiés conformément aux

procédures en vigueur.

7.05 - Direction des ressources matérielles

La Direction des ressources matérielles a la responsabilité de :

7.05.1 S'assurer qu'un mécanisme de sécurité garantissant la gestion rigoureuse des accès, en collaboration avec les services ou départements concernés, protège les zones où se trouvent des actifs informationnels contenant de l'information critique ou délicate. Ces zones devront être sécurisées et accessibles uniquement aux personnes qui en ont spécifiquement besoin, en raison de leur fonction, pour accomplir leurs tâches ;

7.05.2 S'assurer que l'ensemble du site est adéquatement protégé par des contrôles appropriés ;

7.05.3 S'assurer que les actifs informationnels sont protégés contre les menaces environnementales, les désastres naturels, les pannes, les bris, les sinistres, etc.

7.06 - Direction des technologies de l'information

La Direction des technologies de l'information a la responsabilité de :

7.06.1 Fournir à chaque utilisateur ou utilisatrice ses propres accès, avec les permissions et droits correspondants, à l'infrastructure informatique ainsi qu'aux réseaux filaires et sans-fils du Collège. L'utilisation de comptes génériques est à proscrire ;

7.06.2 Mettre en place les sous-réseaux appropriés et s'assurer que chaque personne n'a accès qu'à ceux dont elle a besoin et pour lesquels elle bénéficie d'une autorisation ;

7.06.3 Sensibiliser la communauté aux bonnes pratiques de sécurité de l'information, notamment quant à la gestion des mots de passe, et s'assurer de la disponibilité d'un gestionnaire de mots de passe lorsque nécessaire ;

7.06.4 Soutenir les pilotes de système d'information dans la gestion des identités et des accès ;

7.06.5 Activer, pour les systèmes critiques et sensibles qui le permettent, l'authentification à deux facteurs ;

7.06.6 S'assurer que tous les logiciels à accès privilégiés, c'est-à-dire ceux qui peuvent modifier ou transférer un gros volume d'information facilement, sont utilisés exclusivement à l'aide de comptes à privilèges spéciaux ;

7.06.7 Établir une authentification et un annuaire d'identité uniques, là où les systèmes le permettent, et ainsi harmoniser les différentes méthodes d'authentification, sur les plateformes infonuagiques ou au Collège, afin d'avoir une vue globale des accès de chaque identité ;

7.06.8 Gérer les accès des comptes de service et des comptes d'application en modifiant les identifiants par défaut (nom, usager et mot de passe) et en appliquant le principe du moindre privilège ;

7.06.9 Configurer les audits nécessaires, par exemple les rapports, alertes et suivis ;

7.06.10 Assurer une redondance en ce qui a trait au réseau et vérifier que le câblage est protégé ;

7.06.11 Veiller à ce que les équipements utilisés hors site soient sécurisés en fonction des risques et que chaque retrait d'équipement soit dument autorisé ;

7.06.12 Veiller à ce que les équipements, à la fin de leur vie utile, soient détruits par logiciel effaceur, démagnétisation ou par destruction physique ;

7.06.13 Préconiser le principe du moindre privilège lors de la création de comptes d'utilisation dans une base de données. Les utilisateurs et utilisatrices de la base de données devraient avoir uniquement les privilèges minimums nécessaires et utiliser les autorisations les plus strictes possibles sur tous les objets de base de données, telles que la simple exécution d'interfaces (ex : procédures stockées, vues, etc.) mises à leur disposition ;

7.06.14 S'assurer que les logiciels s'exécutent selon le principe du moindre privilège pour accomplir les tâches nécessaires. Lorsque c'est possible, des comptes isolés avec des privilèges limités à une tâche spécifique doivent être créés.

7.07 - Secrétariat général et direction des affaires juridiques

Le Secrétariat général et la direction des affaires juridiques a la responsabilité de :

7.07.1 S'assurer que le Collège et ses prestataires de services externes prennent les mesures nécessaires à l'application et au respect des lois et règlements en matière de protection des renseignements personnels ;

7.07.2 Conseiller et sensibiliser les utilisateurs et utilisatrices en matière de protection des renseignements personnels et d'accès à l'information ;

7.07.3 S'assurer que la présente Directive soit transmise à chaque prestataire de services externe ayant accès aux actifs informationnels du Collège, selon les prescriptions de la Politique sur l'utilisation des technologies de l'information (PO-27) et de la Politique de sécurité de l'information (PO-33).

ARTICLE 8.00 — RESPONSABLE DE LA DIRECTIVE

La Direction des technologies de l'information est responsable de l'application et de la diffusion de la Directive.

ARTICLE 9.00 — ENTRÉE EN VIGUEUR ET RÉVISION

9.01 - Entrée en vigueur

La présente Directive entre en vigueur au moment de son adoption par le Comité de direction du Collège.

9.02 - Révision

La révision et la mise à jour de la Directive sont prévues au besoin, ou au plus tard tous les cinq (5) ans.