COLLÈGE
ANDRÉ-GRASSET

Politique de gestion des identités et des accès (GIA)

Mai 2025

Table des matières

1. INTRODUCTION

Cette politique, dédiée à tous les intervenants en lien avec la **G**estion des **I**dentités et des **A**ccès, précise les règles de gestion déterminées dans notre organisation, les rôles et responsabilités de chacun pour le bon fonctionnement des opérations et le détail des actions à poser selon les évènements (voir point 5).

Cette politique touche le personnel enseignant et non enseignant du Collège André-Grasset et de l'Institut Grasset ainsi que les étudiants.

La politique applique les deux principes suivants : un minimum de comptes actifs et un accès minimal mais fonctionnel à chacun, ce qui correspond aux bonnes pratiques en cybersécurité et en protection des renseignements personnels. Toute dérogation à ces normes doit être préautorisée par le Directeur des finances et des services administratifs ou le Coordonnateur des technologies de l'information.

2. TERMINOLOGIE

AD: Active directory. Service d'annuaire Windows utilisé pour stocker des informations relatives aux ressources réseau sur un domaine. Permet notamment de fournir des services centralisés d'identification et d'authentification à un réseau.

Absence prolongée : 6 semaines consécutives d'absence en ne comptant pas les vacances

DTI : Direction des technologies de l'information

GTI : Groupe Technique d'Intervention

Identité numérique: Se réfère au compte de l'active directory (AD)

3. RÔLE DES INTERVENANTS

3.1 Le service des ressources humaines

- En cas d'embauche, absence prolongée, départ, suspension, remplacement temporaire ou mouvement interne d'un employé, transmets les informations nécessaires au(x) gestionnaire(s) concerné(s) ainsi qu'à la DTI;
- Il fait le suivi des absences de courtes durées répétées afin de déclencher le processus nécessaire si la durée dépasse les 6 semaines (sans compter les vacances);
- Il collabore à la révision annuelle des identités et des accès

3.2 Les gestionnaires

- Complètent la procédure en vigueur aux droits d'accès & équipements requis lors des mouvements de personnel (incluant consultants externes, stagiaires, bénévoles, étudiants salariés, employés…) dans leur service et le transmettent à la DTI. Si connue, la date de fin est indiquée;
- Tout nouveau changement aux droits d'accès & équipement d'un employé doit passer par son gestionnaire;
- Ils font les suivis des accès temporaires et avisent lorsque les accès ne sont plus nécessaires ;
- Ils collaborent à la révision annuelle des identités et des accès.

3.3 Le service des technologies de l'information

- Crée, désactive et supprime les identités numériques et modifie les accès;
- Considère les demandes reçues et transmets aux services concernés les modifications d'accès qui sont gérées par un autre service;
- Ouvre des billets de rappel et fais les suivis en cas d'accès réputés temporaires ou récupération d'équipements;
- Il engage le processus de révision des identités et des accès au mois de mai de chaque année;

3.4 Le service des études

- Fournis au service informatique la liste des étudiants actifs avant le début de la session et lors d'ajout;
- Fournis au service informatique à chaque année la liste des étudiants finissants;
- Fournis au service informatique à chaque année la liste des anciens et des nouveaux étudiants;

4. RÈGLES D'AFFAIRES ET PRATIQUES TECHNOLOGIQUES

Chacune des règles de gestion et bonnes pratiques technologiques de notre organisme a une valeur égale et de ce fait, doit être observée au cours des processus de gestion des identités et des accès. Toute dérogation doit d'abord avoir été autorisée par le Directeur des finances et des services administratifs (DSA) ou la DTI.

4.1 Les comptes pour le personnel

a. Les comptes nominatifs et personnalisés sont favorisés
b. Les comptes d'utilisateur temporaires ou à contrat doivent préférablement avoir une date de péremption préprogrammée.
c. Un compte nominatif du collège sera créé dans les cas suivants :
    i. Employé
    ii. Enseignant
    iii. Chargé de cours
    iv. Remplacement temporaire (employé ou enseignant)
    v. Ancien étudiant salarié
    vi. Étudiants salariés (l'étudiant aura ainsi un compte étudiant et un compte employé)
    vii. Entraineur (sur demande du gestionnaire)
    viii. Membre du conseil d'administration
    ix. Stagiaire (sur demande du gestionnaire)
    x. Bénévole (sur demande du gestionnaire)
d. Un compte nominatif du collège ne sera pas créé dans les cas suivants :
    i. Bénévole et invité
    ii. Étudiant d'un jour
e. Les comptes génériques sont à proscrire. Dans le cas où il s'agit d'une mesure obligatoire pour le fonctionnement de l'organisation, s'assurer de :
    i. Prioriser la création d'une boîte partagée plutôt qu'un profil
    ii. Restreindre le nombre de personnes ayant accès à ce compte
    iii. Supprimer les utilisateurs qui n'ont plus à utiliser ce compte lors de la révision
f. La demande de création de comptes doit être faite par le gestionnaire en suivant le processus en vigueur

4.2 Les demandes d'accès et leur autorisation pour le personnel

a. Les demandes doivent être acheminées
    i. Via le formulaire afférant lors de l'embauche
    ii. Via le système de requêtes à tout autre moment
b. Toutes les demandes doivent être effectuées
    i. Par le gestionnaire concerné
    ii. Par un gestionnaire du GTI

iii. Par le Directeur des finances et services administratifs

c. L'accès à certains fichiers doit contenir le niveau d'accès.
    i. Lecture seulement
    ii. Écriture (modification possible)
    iii. Contrôle total (suppression possible avec risques associés)
d. En cas d'absence d'un responsable des accès, il revient au Directeur des ressources humaines d'autoriser les changements de droits
e. Équipes Teams (Sharepoint)
    i. L'accès aux équipes Teams doit suivre les règles de gouvernance des équipes Teams (voir Annexe B)

4.3 Assignation / modification des accès pour le personnel

a. Appliquer le principe des droits minimaux
b. Dans le cas des fournisseurs, restreindre l'accès en fonction des besoins (ex. wifi et VLAN indépendant)
c. S'assurer d'avoir l'autorisation du gestionnaire avant d'assigner les droits
d. Dans le cas d'un mouvement interne, le changement des anciens accès sera retiré 4 semaines après la nomination du nouvel employé (à moins d'une exception validée par un gestionnaire du GTI)
e. Équipe Teams (Sharepoint)
    i. Le changement d'accès aux équipes Teams doit suivre les règles de gouvernance des équipes Teams (voir Annexe B)
f. Pour un enseignant qui n'a pas d'activité au collège, l'accès sera restreint (ex. licence Office A3 à A1). Les communications des ressources humaines avec cet enseignant se feront à partir du courriel personnel de l'employé.

4.4 Révocation des accès / suppression des identités pour le personnel

a. En cas d'absence prolongée
    i. L'identité numérique et les accès sont préservés
b. En cas de suspension
    i. L'identité numérique globale et les comptes liés aux applications pourraient être désactivés si la situation le nécessite. Au moment de la date de retour prévue, le GTI réactive les comptes après avoir reçu la confirmation du service RH.
c. En cas de retraite
    i. L'identité numérique et les accès sont désactivés en fonction de la fiche de départ rempli par le gestionnaire.
    ii. Une identité numérique inactive sera supprimée lors la prochaine période de révision annuelle
d. En cas de congédiement
    i. L'identité numérique globale et les comptes liés aux applications sont immédiatement désactivés.
e. En cas de départ définitif (démission, décès)
    i. Dès la date de départ, les accès sont suspendus et les identités numériques sont conservées. Les identités pourront être supprimées lors de la révision annuelle. En cas de besoin, une boîte partagée pourra être créée.

ii. En cas de démission, le gestionnaire peut déterminer que l'identité numérique et les accès constituent une menace pour la sécurité informatique et l'intégrité des documents et ainsi demander une désactivation immédiate de l'identité numérique et des accès.

f. En cas d'absence prolongée, retraite, congédiement ou départ définitif, l'utilisateur doit rapporter rapidement les équipements technologiques qui lui ont été prêtés. Idéalement, il les remettra au maximum à sa dernière journée travaillée. Sinon en cas exceptionnel, une entente pourra être prise.
g. Les identités numériques sont détruites au moment de la révision des accès si la désactivation de l'identité numérique a eu lieu il y a plus de 6 mois.
h. Équipes Teams (Sharepoint)
    i. La suppression des accès aux équipes Teams doit suivre les règles de gouvernance des équipes Teams (voir Annexe B)
i. Pour un enseignant, l'identité numérique sera supprimée après la période de rappel (5 ans)
j. Pour un chargé de cours (Institut) l'identité numérique sera supprimée après 2 ans sans charge de cours.

4.5 Normes technologiques pour le personnel

a. L'authentification multi facteurs est activée sur tous les comptes.
b. Stratégie de mots de passe
    i. Utiliser un mot de passe différent pour chaque compte, chaque service
    ii. Mot de passe de 12 caractères contenant au moins une minuscule, une majuscule, un chiffre et un caractère spécial
    iii. Changer les mots de passe au moindre soupçon
    iv. Ne jamais communiquer un mot de passe à un tiers
c. Le nombre maximum de connexions simultanées est de 4 pour les comptes sauf pour les laboratoires
d. Les identités numériques sont automatiquement désactivées après 5 tentatives de connexion infructueuses
e. Les postes de travail sont verrouillés après 60 minutes d'inactivité
f. À moins d'exception analysée et autorisée par un gestionnaire du service des technologies, l'accès administrateur local aux postes de travail est proscrit

4.6 Identité numérique, accès et normes technologiques pour les étudiants

a. Une identité numérique est créée pour chaque étudiant
b. L'identité numérique et les accès d'un étudiant qui a abandonné seront désactivés
c. L'identité numérique d'un étudiant qui n'est plus au collège depuis 2 ans sera supprimée
d. L'identité numérique et les accès d'un étudiant finissant seront désactivés
e. Équipes Teams (Sharepoint)
    i. L'accès et la suppression des équipes Teams suivent la règle de gouvernance des équipes Teams (voir Annexe B)
f. L'authentification multi facteurs est activée sur tous les comptes dans la mesure du possible
g. Stratégie de mot de passe

i. Un mot de passe unique est donné aux étudiants en début de parcours.
ii. Mot de passe de 10 caractères contenant au moins une minuscule, une majuscule, un chiffre et un caractère spécial

5. LES ACTIONS SELON LES ÉVÉNEMENTS

Ce tableau détaille les processus les plus courants. En cas d'exception, il est recommandé de s'enquérir auprès de la DTI, sinon le Directeur des finances et des services administratifs (DSA)

Évènement	Type d'utilisateur	Actions
Embauche	Soutien / Professionnel / Cadre / Enseignant / Étudiant salarié / Stagiaire salarié	**Service RH** • Crée le compte dans Clara (RH-Paie) • Crée le formulaire afférant **Gestionnaire** • Indique le besoin en termes d'accès et d'autorisation en complétant le formulaire afférent. **Service TI** • Crée l'identité numérique • Octroie les accès requis et autorisés • Transmets les informations de connexion au courriel personnel de l'employé • Transmets une confirmation de l'envoi des accès au gestionnaire et au RH • Prépare les équipements à prêter (portable, installation de logiciels, etc.) • Fais signer le contrat de prêt de portable • Installation de la station d'accueil
Réembauche	Enseignant	**Service RH** • Réactive le compte dans Clara (RH-Paie) • Crée un formulaire de réembauche **Service TI** • Valide l'identité numérique • Mettre les accès • Prépare les équipements à prêter (portable, installation de logiciels, etc.) • Fais signer le contrat de prêt de portable • Installation de la station d'accueil
Arrivée/départ	Membre du conseil d'administration	**Service RH** • Lors de l'arrivée d'un membre du CA, la Direction générale demande au service TI la création d'un

		compte. La demande de retrait des accès sera aussi faite par la Direction générale suite à un départ. **Service TI** • Création de l'identité numérique • Transmets les informations de connexion au courriel personnel du membre • Transmission de la confirmation de l'envoi des accès aux RH
Début contrat	Consultant externe	**Gestionnaire** • Envoi d'un courriel au coordonnateur des technologies avec les informations essentielles (type d'accès, raison, début, fin) **Coordonnateur des technologies:** • Vérifie si une identité et/ou des accès seront donnés **Service TI (si accepté)** • Crée l'identité numérique (au besoin) • S'assure que les autorisations sont conformes • Ajoute les accès demandés • Donne les informations au consultant externe ou au gestionnaire qui le donnera au consultant externe • Prends en note la date de fin • À la date de fin, vérifie avec le gestionnaire si l'identité et/ou les accès peuvent être supprimés
Mouvement interne	Même catégorie d'emploi	**Service RH** • Transmets les informations nécessaires aux 2 gestionnaires • Crée le formulaire de mouvement interne **Gestionnaire - *responsable de la nouvelle assignation*** • Remplis le formulaire afférant • Il spécifie si les droits de l'ancien poste doivent être retirés maintenant ou maximum dans 4 semaines **Service TI** • Ajuste les droits comme requis et, s'il y a lieu, se crée un événement de suivi qui sera à traiter X semaines plus tard • À l'échéance de l'événement de suivi, confirme avec le gestionnaire que les droits originaux peuvent être retirés. Renouvelle l'événement de suivi en cas de prolongation temporaire
	Nouvelle catégorie d'emploi	Comme pour un mouvement interne sans changement de catégorie d'emploi **Service TI**

		• En date d'entrée en application du changement, modification de la liste de distribution interne
Absence prolongée	Tous types	**Gestionnaire** • Aviser les RH **Service RH** • Informe le gestionnaire/responsable départemental et le service TI • Avise l'employé que les équipements prêtés doivent être retournés à l'accueil **Service TI** • Documente et retire les accès selon xyz, • Si la date de retour est connue, crée un événement de suivi de réassignation des accès • Une fois réception du matériel, on marque la fin du prêt
Suspension	Tous types	**Service RH** • Avise immédiatement par courriel le service TI de désactiver l'identité numérique de l'employé concerné en indiquant la date de retour prévue **Service TI** • Désactive le compte global et les comptes applicatifs • Ajuste l'identité numérique pour s'assurer qu'elle ne soit pas réactivée (par inadvertance) • Si possible, bloque aussi l'utilisation du portable • Crée un événement de suivi à traiter au moment de la date de retour prévue
Démission / retraite	Tous types	**Gestionnaire** • Aviser les RH **Service RH** • Transmets les informations de départ au service TI et au gestionnaire/responsable départemental • Avise l'employé que les équipements prêtés doivent être retournés aux RH **Service TI, *au lendemain de la date de fin d'emploi*** • Désactive l'identité numérique selon les règles d'affaires internes • Détruis les comptes applicatifs • Récupère les équipements **Gestionnaire de l'employé** • S'il détermine une menace informatique ou informationnelle potentielle, il demande au service TI de désactiver immédiatement les accès et l'identité numérique.

Congédiement	Tous types	**Service RH** • Avise immédiatement le service TI de désactiver l'identité numérique de l'employé concerné • Avise l'employé que les équipements prêtés doivent être retournés aux RH **Service TI** • Désactive l'identité numérique et retire tous les accès aux différents systèmes • Ajuste l'identité numérique pour s'assurer qu'elle ne soit pas réactivée (par inadvertance) **Gestionnaire** • Informe le service TI des particularités relatives à mettre en place (ex. accès aux courriels, aux documents, etc.) **Service TI** • Mets en place les particularités à mettre en place (ex. accès aux courriels, aux documents, etc.)
Nouveaux étudiants	Étudiants	**Service des études** • Extraction d'une liste des nouveaux étudiants et d'une liste de mises à jour • Envoie des listes au service TI **Service TI** • Création des comptes • Envoie du mot de passe au courriel de l'étudiant
Diplomation des étudiants	Étudiants	**Service des études** • Extraction d'une liste des étudiants finissants • Envoie de la liste au service TI **Service TI** • Désactivation des comptes
Étudiants abandonnent leurs cours	Étudiants	**Service des études** • Extraction d'une liste des étudiants ayant abandonné leurs études • Envoie de la liste au service TI **Service TI** • Désactivation des comptes
5 ans sur la liste de rappel	Enseignant	**Service TI** • Sors la liste annuelle de g-profs et la liste de rappel TI

		Ressources humaines • Indique les enseignants qui ne sont plus dans la liste de rappel **Service TI** • Supprime les comptes en question
2 ans sans cours	Chargé de cours (Institut)	**Service TI de l'Institut** • Sors la liste des chargés de cours **Coordonnateurs de programme** • Indique les enseignants qui n'ont pas donné de cours dans les 2 dernières années **Services TI** • Supprime les comptes en question

6. RÉVISION DES IDENTITÉS ET DES ACCÈS

La révision des identités et des accès permet notamment d'identifier les comptes orphelins. La suppression de ces comptes diminue le risque associé à leur maintien et permet ainsi d'améliorer la posture de cybersécurité du Collège.

Elle est effectuée une fois l'an (sauf aux 2 ans pour les comptes génériques), au mois de mai et se décline comme suit :

1. Les TI exportent ces listes d'utilisateur de l'AD
    - Enseignants
    - Enseignants de la liste de rappel
    - Employés
    - Comptes génériques
    - Chargés de cours (Institut)

2. Les TI envoient les listes à la DTI et au Directeur des ressources humaines (Collège) ou aux coordonnateurs de programme (Institut)

3. La DRH ou le coordonnateur met en rouge les comptes à supprimer. La DRH met en orange les enseignants sur la liste de rappel.

4. Le gestionnaire indique les comptes génériques à supprimer ou désactiver

5. La DRH envoie les listes au DSA pour validation.

6. Le DSA envoie les listes au GTI (dont le coordonnateur).

7. Le GTI supprime, désactive ou en restreint les accès selon ce qui a été déterminé auparavant (ex. nouveaux enseignants sur la liste de rappel qui passent de licences A3 à A1).

7. Les annexes

ANNEXE A – Lettre de confidentialité pour les consultants externes

COLLÈGE ANDRÉ-GRASSET

Lettre de confidentialité – consultants externes

Entre les parties :
Le **Collège André-Grasset**, ci-après désigné comme « l'Organisation »,
Et **[Nom de la personne ou entité]**, ci-après désigné comme « l'Utilisateur »,

Article 1 : Objet de l'engagement
L'Organisation met à disposition de l'Utilisateur une identité numérique ainsi que certains accès à ses systèmes dans le cadre des activités suivantes : [Précisez les activités ou le rôle].
En signant cette lettre, l'Utilisateur s'engage à respecter la confidentialité des informations accessibles, à utiliser les accès fournis de manière responsable et conforme aux politiques internes (notamment la Politique relative à l'utilisation des technologies de l'information, des communications et des médias sociaux), et à protéger l'intégrité des données et systèmes.

Article 2 : Définition des informations confidentielles
Par "informations confidentielles", on entend:

- Toute donnée, information ou document lié aux activités, aux employés, aux étudiants, aux partenaires ou aux systèmes du Collège André-Grasset ;
- Toute information protégée par la Loi sur la protection des renseignements personnels ou d'autres cadres juridiques applicables (ex. loi 25).

Renseignement personnel selon Éducaloi « c'est un renseignement qui permet de vous identifier, directement ou indirectement, en tant que personne. Ces renseignements sont notamment liés à votre situation sociale et familiale, votre santé, vos finances et votre travail. En voici quelques exemples:

- prénom et nom,
- adresse résidentielle,
- adresse courriel personnelle,
- numéro de téléphone,
- âge,
- état civil,
- numéro de permis de conduire »

Source : https://educaloi.qc.ca/capsules/la-protection-de-vos-renseignements-personnels/

Article 3 : Engagements de l'utilisateur
L'Utilisateur s'engage à :

1. **Utiliser les accès exclusivement pour les activités autorisées** et ne pas partager ses identifiants avec une tierce partie.
2. **Protéger ses identifiants et dispositifs** (mots de passe, cartes d'accès, etc.) contre toute perte ou vol.
3. **Préserver la confidentialité des informations** accessibles via les systèmes, sauf autorisation expresse de l'Organisation.
4. **Informer immédiatement l'Organisation** de tout incident, comme une violation de sécurité, un accès non autorisé ou une perte d'informations sensibles.
5. **Restituer ou détruire** toute information confidentielle à la fin de la relation ou sur demande de l'Organisation.

Article 4 : Conséquences en cas de non-respect
En cas de non-respect des engagements mentionnés, l'Organisation se réserve le droit de :

- Révoquer immédiatement les accès numériques et suspendre tout privilège associé ;
- Entreprendre des mesures légales, si nécessaire.

Article 5 : Durée et résiliation
Cet engagement entre en vigueur à compter de la date de signature et reste applicable pendant toute la durée de l'accès aux systèmes de l'Organisation. L'Utilisateur reste soumis à cette obligation de confidentialité même après la fin de sa relation avec l'Organisation.

Article 6 : Acceptation et signature
En signant ce document, l'Utilisateur reconnaît avoir pris connaissance des responsabilités associées à l'utilisation des accès fournis et s'engage à respecter les termes ci-dessus.

Signature de l'Utilisateur :
Nom : _____
Signature : _____
Date : _____

Signature du représentant de l'Organisation :
Nom : _____
Titre : _____
Signature : _____
Date : _____

ANNEXE B – Règles de gouvernance des équipes Teams (Sharepoint)

La gestion et le contrôle des accès sont sous la responsabilité du propriétaire de l'équipe TEAMS. Pour les personnes étudiantes et enseignantes, ce rôle est automatiquement assigné à la personne qui crée l'équipe. Pour le personnel administratif, la création d'une équipe se fait par l'entremise du système de requête. Le gestionnaire de la direction ou du service à laquelle l'équipe est destinée est alors désignée propriétaire de l'équipe. L'administrateur SharePoint agit en soutien auprès des propriétaires d'équipes au besoin.

Catégorie	Étudiante	Enseignante	Personnel administratif
Fonction de l'équipe	Activités étudiantes	Activités d'enseignements	Activités administratives
Création d'une équipe	Permise	Permise	Système de requête
Création des canaux	Permise	Permise	Propriétaire seulement
Désignation du propriétaire	Assignée à la personne qui crée l'équipe	Assignée à la personne qui crée l'équipe	Assignée au gestionnaire de la direction ou du service
Désignation des co-propriétaires	Autorisée, facultative	Autorisée, facultative	Autorisée. Il est fortement recommandé d'avoir un 2e propriétaire
Ajout des membres	Oui	Oui	Oui, en fonction des besoins et du niveau de confidentialité de l'équipe
Ajout des invités (adresse courriel externe)	Permis	Permis	Permis, en fonction des besoins et du niveau de confidentialité de l'équipe
Retrait des membres	Facultatif	Recommandé	Obligatoire
Retrait des invités	Facultatif	Recommandé	Obligatoire
Retrait des co-propriétaires	Facultatif	Recommandé	Obligatoire. Dois désigner un nouveau co-propriétaire
Autorise ou refuse une demande d'accès	Oui	Oui	Oui