

POLITIQUE N° 23

POLITIQUE DE SÉCURITÉ DE L'INFORMATION NUMÉRIQUE

La présente politique a été adoptée pour la première fois en application de la résolution numéro 386-09, qui est entrée en vigueur le

1^{er} juin 2018

En cas de divergence, la version anglaise prévaut sur la version française.

POLITIQUE NO 23 - POLITIQUE DE SÉCURITÉ DE L'INFORMATION NUMÉRIQUE

Table des matières

ARTICLE 1- PRÉAMBULE	1
ARTICLE 2- OBJECTIFS	1
ARTICLE 3 - CADRE LÉGAL ET ADMINISTRATIF	2
Article 4 CHAMP D'APPLICATION	2
ARTICLE 5 - PRINCIPES DIRECTEURS	3
ARTICLE 6 – CADRE DE GESTION	4
6.1 Gestion de l'accès	4
6.2 Gestion des risques	4
6.3 Gestion des incidents	5
ARTICLE 7 - RÔLES ET RESPONSABILITÉS	5
7.1 Conseil d'administration	5
7.2 Direction générale	5
7.3 Groupe de travail sur la sécurité de l'information	6
7.4 Directeur général	6
7.5 Responsable de la sécurité de l'information (RSI)	7
7.6 Coordonnateur sectoriel de la gestion des incidents (« CSGI »)	7
7.7 Services des technologies de l'information (« STI »)	8
7.8 Services de gestion des installations (« SGI »)	9
7.9 Services des ressources humaines (« SRH »)	9
7.10 Responsable d'actifs informationnels (« RAI »)	9
7.11 Utilisateurs	10
ARTICLE 8 - SENSIBILISATION ET INFORMATION	10
Article 9 SANCTIONS	11
ARTICLE 10 - DIFFUSION ET MISE À JOUR DE LA PRÉSENTE POLITIQUE	11
ARTICLE 11 - ENTRÉE EN VIGUEUR	11
Annexe A	12

POLITIQUE N^o 23 - POLITIQUE DE SÉCURITÉ DE L'INFORMATION NUMÉRIQUE

ARTICLE 1- PRÉAMBULE

La présente politique permet au Cégep John Abbott (le « **Cégep** ») de remplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information numérique qu'il crée, qu'il reçoit ou qu'il détient dans le cadre de ses activités, qu'elle soit conservée par le Cégep lui-même ou par un tiers (collectivement, l'« **information** »). Cette information peut exister sous plusieurs formes électroniques. Il peut s'agir de renseignements personnels des étudiantes et étudiants et du personnel, de renseignements professionnels faisant l'objet de droits de propriété intellectuelle (enseignants et chercheurs) et d'information stratégique ou opérationnelle du Cégep.

Le monde numérique n'a pas de frontières et est ouvert aux pirates des temps modernes. Ces personnes, cachées dans l'espace virtuel, recherchent les vulnérabilités des systèmes afin d'accéder à divers types d'information et de les utiliser à leur profit. Notre Cégep, en tant que membre du réseau de l'enseignement supérieur, a une image publique et constitue donc une cible potentielle.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, G-1.03) (la « **LGGRI** ») et de la *Directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du Trésor du Québec applicable aux cégeps) (la « **DSI** ») crée des obligations qui incombent aux cégeps en leur qualité d'organismes publics. À cet égard, la DSI oblige les cégeps à adopter et à mettre en œuvre une politique de la sécurité de l'information - dont les principaux termes sont définis dans la DSI – à maintenir à jour cette politique et à en assurer l'application, principalement par l'utilisation de processus formels de sécurité de l'information pour gérer les risques, l'accès à l'information et les incidents.

ARTICLE 2- OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter de ses obligations en matière de sécurité de l'information. Plus précisément, le Cégep doit veiller à :

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et seulement par les personnes autorisées;
- l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation et ce que le support de cette information lui procure la stabilité et la pérennité voulues;
- la confidentialité de l'information, en limitant la communication et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, le Cégep met en place la présente politique dans le but d’orienter et de déterminer sa démarche en matière de sécurité des TI. La présente politique renforce les processus de contrôle interne en fournissant une assurance raisonnable du respect de la législation et des directives gouvernementales, ainsi que d'autres exigences de réduction des risques liés à la protection de l’information.

ARTICLE 3 - CADRE LÉGAL ET ADMINISTRATIF

La présente politique s'inscrit dans un contexte régi notamment par ce qui suit :

- la *Charte des droits et libertés de la personne* (LRQ, C-12);
- le *Code civil du Québec* (LQ, 1991, 64);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *LGRI*;
- la *Loi concernant le cadre juridique des technologies de l'information* (LRQ, C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, A-2.1);
- la *Loi sur les archives* (LRQ, A-21.1);
- le *Code criminel* (LRC, 1985, C-46);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (A-2.1, r. 2
- la *DSI*;
- la *Loi sur le droit d'auteur* (LRC, 1985, C-42);
- la *Politique n° 9 du Cégep John Abbott (Gestion des documents et archives)*;
- la *Politique n° 20 du Cégep John Abbott (Cadre de gestion des risques)*;
- la *Politique n° 21 du Cégep John Abbott (Communications)*;

Article 4 CHAMP D'APPLICATION

La présente politique s'applique à tous les utilisateurs de l'information, c'est-à-dire à toutes les personnes physiques ou morales qui, en tant qu’employés, consultants, partenaires, fournisseurs, étudiantes et étudiants ou membres du grand public, utilisent les actifs informationnels du Cégep.

ARTICLE 5 - PRINCIPES DIRECTEURS

Les principes directeurs qui guident le Cégep en matière de sécurité de l'information sont les suivants :

- a) l'information à protéger doit être bien connue en identifiant les personnes qui en sont responsables ainsi que les caractéristiques de l'information à protéger (il est donc important de tenir à jour l'inventaire des actifs informationnels);
- b) les normes internationales pertinentes sont utilisées pour favoriser la mise en place de pratiques exemplaires et pour recourir à des barèmes de comparaison avec des organismes ou établissements similaires;
- c) une approche fondée sur le risque acceptable est adoptée (permettant l'évaluation des niveaux de risque et la mise en œuvre d'une combinaison de mesures raisonnables pour garantir la sécurité de l'information, à un coût proportionné à la sensibilité de l'information et aux effets négatifs potentiels en cas de compromission de l'information);
- d) l'importance de la présente politique est reconnue et cette politique est gérée par une équipe compétente et de taille appropriée (cette équipe doit définir, mettre en place, exercer et ajuster la gestion de la sécurité de l'information);
- e) les renseignements personnels et autres renseignements confidentiels sont rigoureusement protégés;
- f) l'environnement technologique est reconnu comme étant en constante évolution et interconnecté avec le monde; la sécurité de l'information doit pouvoir s'adapter aux changements de l'environnement technologique;
- g) il faut reconnaître l'importance d'une évaluation régulière des risques, de la mise en place de mesures proactives de sécurité et de méthodes de détection d'usage abusif ou inapproprié de l'information, de la définition de méthodes d'élimination des menaces ou de récupération des données compromises;
- h) l'information doit être protégée tout au long de son cycle de vie, depuis son acquisition ou sa création jusqu'à sa destruction; le niveau de sécurité peut varier au cours du cycle de vie de l'information;
- i) les principes de partage des pratiques exemplaires et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics sont à privilégier;
- j) il est impératif d'adopter une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle; chaque personne ayant accès à l'information est responsable du respect de la confidentialité, de la disponibilité et de l'intégrité de l'information;
- k) chaque employé a accès à l'information minimale nécessaire à l'exercice de ses tâches normales;

- l) il y a une communication transparente sur les menaces pesant sur les actifs informationnels afin de faciliter la compréhension de l'importance de l'application des mesures de sécurité prescrites et d'être informé de manière à reconnaître les incidents de sécurité et à agir en conséquence;
- m) un plan de continuité des activités permettant de rétablir en temps opportun les services essentiels à la clientèle doit être mis en place.

ARTICLE 6 – CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents intéressés du Cégep par la mise en place de la présente politique qui permet une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être revues périodiquement pour tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces, des risques et des vulnérabilités.

La présente politique s'articule autour de trois axes fondamentaux de gestion. Il s'agit de la gestion de l'accès, de la gestion des risques et de la gestion des incidents.

6.1 Gestion de l'accès

L'accès aux différents systèmes doit être géré et contrôlé pour faire en sorte que l'accès, la communication et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises pour protéger l'intégrité et la confidentialité des données et renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution des responsabilités et sur l'obligation de rendre compte à tous les niveaux de personnel du Cégep. À cet égard, voir l'annexe A qui fait partie intégrante de la présente politique.

6.2 Gestion des risques

Une catégorisation des « actifs informationnels à jour » soutient l'analyse des risques en permettant de connaître la valeur de l'information à protéger.

L'analyse des risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en précisant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Cégep. Les risques à portée gouvernementale sont déclarés conformément à la DSI.

Le niveau de protection de l'information est établi en fonction de ce qui suit :

- la nature de l'information et son importance;
- la probabilité d'un incident, d'une erreur ou d'une malveillance à laquelle elle pourrait être exposée;
- les conséquences de la réalisation de ces risques;
- le niveau de risque acceptable pour le Cégep.

6.3 Gestion des incidents

Le Cégep déploie des mesures de sécurité de l'information afin d'assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'atteinte des objectifs suivants :

- limiter la probabilité d'occurrence d'incidents en matière de sécurité de l'information;
- gérer adéquatement ces incidents afin d'en minimiser les conséquences et, s'il y a lieu, de rétablir les opérations.

Les incidents liés à la sécurité de l'information de portée gouvernementale doivent être déclarés conformément à la DSI (au CERT/AQ).

Dans la gestion des incidents, le Cégep peut exercer ses pouvoirs et prérogatives à l'égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

ARTICLE 7 - RÔLES ET RESPONSABILITÉS

La présente politique confie la gestion de la sécurité de l'information du Cégep à des instances, à des comités et à des personnes en raison des fonctions particulières qu'ils exercent.

7.1 Conseil d'administration

Le conseil d'administration adopte la présente politique et ses modifications éventuelles. Le conseil est informé des actions du Cégep en matière de sécurité de l'information. Il s'agit du chef de l'organisation chargée de l'application de la présente politique.

Le comité exécutif et/ou tout autre comité du conseil d'administration peuvent prendre des décisions dans un cadre préalablement déterminé par le conseil d'administration.

7.2 Comité de direction

Le comité de direction détermine les mesures visant à favoriser la mise en œuvre de la présente politique et des obligations légales du Cégep en matière de sécurité de l'information. Ainsi, elle détermine les orientations stratégiques, les plans d'action et l'évaluation des risques touchant l'information du Cégep.

Elle peut également déterminer des lignes directrices et des procédures qui clarifient ou soutiennent l'application de la présente politique.

7.3 Groupe de travail sur la sécurité de l'information

Le groupe de travail sur la sécurité de l'information a pour objectif d'aider le responsable de la sécurité de l'information (**RSI**) à mettre en œuvre la présente politique et d'autres éléments qui pourraient être nécessaires pour veiller à ce que le Cégep soit protégé et respecte les règlements en vigueur. Il s'agit d'un groupe de travail tactique et opérationnel qui se réunit au besoin.

Ce comité est notamment chargé des plans d'action et des bilans de sécurité de l'information, des mesures de sensibilisation ou de formation et de toute proposition d'action en matière de sécurité de l'information. C'est aussi une tribune d'échanges entre les intéressés ou d'observation de l'évolution du projet de sécurité de l'information.

Le comité sera composé des principaux intéressés du Cégep qui prendront directement part à la sécurité de l'information.

Ce comité sera composé des personnes suivantes : le RSI, le directeur des STI, les principaux propriétaires de données (le directeur du SRH, le directeur des finances, le registraire), le CSGI, le responsable des opérations et de la sécurité des STI, le spécialiste de la sécurité (le cas échéant) et responsable de l'infrastructure des STI.

7.4 Directeur général

Le directeur général veille à l'application de la présente politique.

Le directeur général est chargé de ce qui suit:

- superviser le RSI dans l'exercice de son mandat;
- déléguer au secrétaire général certaines responsabilités en matière de gestion de l'information;
- faire en sorte que le conseil d'administration adopte des orientations stratégiques, des évaluations des risques, des plans d'action, des évaluations de la sécurité, la reddition de compte en matière de sécurité de l'information;
- autoriser (à titre exceptionnel) une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement lié à la mission du Cégep;
- autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la présente politique;
- tenir un registre des exemptions et un registre des cas de violation de la présente politique.

7.5 Responsable de la sécurité de l'information (RSI)

La fonction de RSI est déléguée à un cadre dirigeant par le conseil d'administration. Dans le cas du Cégep, il s'agit du directeur des STI. Le RSI relève du directeur général au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Cette personne veille à ce que le niveau de maturité des pratiques de gestion de la sécurité de l'information réponde aux besoins du Cégep. Cette personne est nommée par le conseil d'administration.

Le RSI :

- élabore et propose le programme de sécurité de l'information du Cégep et rend compte de sa mise en œuvre au comité de direction;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les règles et les bonnes pratiques en matière de sécurité de l'information et propose les mises à jour appropriées de la présente politique;
- assure la coordination et la cohérence des actions du Cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans l'organisation;
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci;
- procède aux enquêtes relatives à des transgressions graves ayant trait en particulier à la présente politique, à la suite de l'autorisation du directeur général;
- s'assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

7.6 Coordonnateur sectoriel de la gestion des incidents (« CSGI »)

Le CSGI collabore étroitement avec le coordonnateur organisationnel de gestion des incidents du réseau du ministère de l'Éducation et de l'enseignement supérieur (MEES) (le « **Réseau COGI** »). La personne qui occupe cette fonction agit de manière tactique et opérationnelle pour fournir un soutien en matière de gestion des incidents et de gestion des risques dans le domaine des TI. Le CSGI est l'interface officielle avec l'Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (« **CERT/AQ** »).

En particulier, le CSGI

1. collabore avec le réseau collégial, le réseau COGI et le RSI de son organisation à l'élaboration des différents éléments stratégiques et tactiques en matière de TI, notamment
 - une politique des TI;
 - un cadre de gestion;
 - un registre des habilitations;
 - la catégorisation des actifs;
 - les mesures de sécurité en ce qui concerne les actifs essentiels;
 - un processus formel de gestion des risques en matière de sécurité de l'information;
 - un processus formel de gestion des droits d'accès à l'information.
2. participe activement à la mise en œuvre par le Réseau COGI du réseau d'alerte en matière de TI et établit des liens avec les autres CSGI afin de favoriser le partage d'expertise et d'éléments tactiques et opérationnels à élaborer et à mettre en œuvre;
3. participe avec le Réseau COGI au processus gouvernemental de gestion des incidents et au réseau gouvernemental d'alerte coordonné par le CERT/AQ ;
4. élabore et met en œuvre, avec le soutien du Réseau COGI, un processus formel de gestion et de déclaration des incidents pour son organisation, y compris un registre des incidents de son organisation;
5. coordonne la gestion des incidents de sécurité des TI de son organisation ayant une incidence à portée gouvernementale avec le soutien du Réseau COGI :
 - met en place, si elle n'existe pas, une équipe d'intervention en cas d'incident (« EII ») dans son organisation;
 - avec les membres de l'EII, élabore, met en œuvre et met à l'essai un plan d'intervention en cas d'incidents de sécurité de son organisation;
6. met en œuvre les stratégies d'intervention appropriées pour le Cégep au moment d'un incident, en collaboration avec le Réseau COGI.

7.7 Services des technologies de l'information (« STI »)

En matière de sécurité de l'information, les STI veillent à ce que les exigences de sécurité de l'information soient satisfaites dans l'exploitation des systèmes d'information de même que dans la réalisation des projets de développement ou d'acquisition de systèmes d'information dans lesquels elles interviennent :

- ils participent activement à l'analyse des risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;

- ils appliquent des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, par exemple l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information pour assurer la sécurité de l'information en question;
- ils participent aux enquêtes relatives à des contraventions réelles ou apparentes à la présente politique, autorisées par le directeur général.

7.8 Services de gestion des installations (« SGI »)

Les SGI, en collaboration avec le RSI, participent à l'identification des mesures de sécurité physique visant à protéger adéquatement les actifs informationnels du Cégep.

7.9 Services des ressources humaines (« SRH »)

En ce qui concerne la sécurité de l'information, les SRH obtiennent de tous les nouveaux membres du personnel du Cégep un engagement à respecter la présente politique.

7.10 Responsable d'actifs informationnels (« RAI »)

Le RAI est le gestionnaire détenant l'autorité au sein d'un service ou d'un département, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation et à la sécurité des actifs informationnels sous la responsabilité de ce service ou département. Il peut donc y avoir plusieurs RAI dans le Cégep. Le RAI peut déléguer sa responsabilité, en tout ou en partie, à un autre membre du service ou du département.

Le RAI est chargé de ce qui suit:

- informer le personnel relevant de son autorité et les tiers avec lesquels le service ou le département collabore, des dispositions de la présente politique dans le but de le sensibiliser à la nécessité de s'y conformer;
- collaborer activement à la catégorisation de l'information du service ou du département sous sa responsabilité et à l'analyse de risques;
- voir à la protection de l'information et des systèmes d'information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés par le personnel autorisé en conformité avec la présente politique;
- veiller à ce que les exigences en matière de sécurité de l'information soient prises en compte dans tout processus d'acquisition et tout contrat de services sous sa responsabilité et veiller à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la présente politique;
- signaler aux STI toute menace ou tout incident afférant à la sécurité de l'information;

- collaborer à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'information;
- signaler au directeur général tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de la présente politique.

7.11 Utilisateurs

La responsabilité de la sécurité de l'information du Cégep incombe à tous les utilisateurs des actifs informationnels du Cégep.

Tout utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

À cette fin, l'utilisateur doit :

- se conformer à la présente politique et à toute autre directive du Cégep en matière de sécurité de l'information et d'utilisation de l'information;
- utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- participer à la catégorisation de l'information de son service ou département;
- respecter les mesures de sécurité mises en place, sans les contourner, ni modifier leur configuration ni les désactiver;
- signaler au responsable des actifs informationnels, tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Cégep;
- collaborer à toute intervention visant à indiquer ou à atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information;

Aussi, tout utilisateur du Cégep doit se conformer aux politiques et aux directives en vigueur au Cégep dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

ARTICLE 8 - SENSIBILISATION ET INFORMATION

La sécurité de l'information repose sur la régulation des comportements et la responsabilisation individuelle. À cet égard, les membres de la communauté collégiale doivent être sensibilisés à ce qui suit :

- les mesures, le programme et la politique de sécurité applicables à l'information du Cégep et à ses systèmes;
- les conséquences d'une atteinte à la sécurité;
- leur rôle et leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation doivent être offertes périodiquement. De plus, des documents explicatifs doivent être disponibles sur le système de diffusion de l'information du Cégep.

Article 9 SANCTIONS

En cas de contravention à la présente politique, l'utilisateur engage sa responsabilité personnelle; il en va de même pour toute personne qui, par négligence ou omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal de la présente politique et aux mesures de sécurité de l'information qui s'y rapportent s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, conformément aux lois ou aux règles disciplinaires internes applicables.

De même, toute contravention de la présente politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme extérieur, est passible des sanctions prévues au contrat qui le lie au Cégep ou en vertu des dispositions de la législation applicable en la matière.

ARTICLE 10 - DIFFUSION ET MISE À JOUR DE LA PRÉSENTE POLITIQUE

Le RSI, assisté de la direction générale, est responsable de la diffusion et de la mise à jour de la présente politique. La présente politique sera réexaminée au plus tard trois (3) ans après son adoption.

ARTICLE 11 - ENTRÉE EN VIGUEUR

La présente politique entrera en vigueur dès son adoption.

Annexe A

Comptes d'utilisateurs

Objectif

La présente annexe a pour objectif d'établir des principes généraux et des règles de fonctionnement pour la gestion des comptes d'utilisateurs et l'accès au système afin de permettre l'utilisation des ressources du Cégep John Abbott (le « **Cégep** »), notamment les services suivants :

- le courrier électronique,
- le système de fichiers et de dossiers du serveur,
- les données stockées localement,
- tout système renfermant des renseignements personnels et privés.

Champ d'application de la présente annexe

La présente annexe s'applique à tout le personnel qui doit avoir accès aux systèmes mentionnés au paragraphe précédent. En outre, la présente annexe s'applique aux fournisseurs externes, entrepreneurs, agences, etc. qui ont un contrat avec le Cégep à des fins de maintenance des logiciels et du matériel informatique, de l'équipement ou à toute autre fin.

Principes directeurs

Les directives suivantes constituent le fondement du présent document :

Le Cégep¹

- n'accorde que les droits d'accès essentiels à l'exécution des tâches liées au travail.
- paramètre les mots de passe pour refléter les pratiques exemplaires dans les directives de sécurité².
- ne permet jamais aux systèmes d'afficher les mots de passe.
- bloque l'accès aux systèmes pendant dix (10) minutes après trois (3) tentatives de connexion infructueuses.
- attribue des mots de passe temporaires lors de l'accès initial aux systèmes.
- contrôle l'utilisation de tous les comptes d'utilisateurs à partir desquels l'accès à l'Internet est possible.
- verrouille les écrans après 15 minutes de non-utilisation, obligeant l'utilisateur à saisir à nouveau son mot de passe avant de se reconnecter.

L'utilisateur a l'obligation de faire ce qui suit :

¹ Chaque fois que le système le permet ou que la fonctionnalité est intégrée.

² Minimum de huit caractères, contenant 3 des 4 groupes suivants : caractères minuscules, caractères majuscules, chiffres et caractères spéciaux.

- modifier son mot de passe lors de son premier accès à un système;
- se connecter aux serveurs JAC et enregistrer les documents liés au travail sur le réseau du Cégep³ ou Office 365 (c.-à-d. One Drive) pour les conserver et les sauvegarder;
- n'utiliser les renseignements personnels et confidentiels qui résident dans nos systèmes qu'à la seule fin du travail du Cégep pour lequel les données sont destinées ou recueillies;
- verrouiller son poste de travail (touche Windows + L)⁴ lorsqu'il n'est pas utilisé s'il est accessible ou situé dans une zone publique;
- utiliser uniquement son propre compte et son propre mot de passe lorsqu'il se connecte à un ordinateur;
- suivre les directives du présent document ainsi que les lignes directrices sur l'utilisation appropriée des ressources informatiques, y compris l'Internet.

Rôles et responsabilités

La direction des services de technologie de l'information (STI)

La direction des STI a les responsabilités suivantes :

- gérer les comptes de réseau et de courrier électronique;
- gérer l'accès à tous les autres comptes, y compris ceux qui étaient historiquement décentralisés⁵, sauf en ce qui concerne un nouveau système actuellement en phase d'essai ou de mise en œuvre préliminaire;⁶
- contrôler et auditer tous les comptes du Cégep;
- contrôler et auditer l'ensemble du trafic Internet;
- générer des rapports d'accès au système pour le responsable des actifs informationnels (le « **RAI** »)⁷;
- valider le statut du membre du personnel auprès du propriétaire des données du système concerné;
- réviser régulièrement la présente annexe.

Les techniciens des STI

Sous la direction d'un gestionnaire des STI et/ou du directeur des services de gestion des installations et des technologies de l'information, les activités générales des techniciens des STI sont les suivantes :

³ Mise en garde : en cas de sinistre informatique ou d'accident, les STI ne seront pas en mesure de vous aider si les documents sont sauvegardés sur un lecteur « c » ou un autre appareil portable.

⁴ L'équivalent pour Mac OSX est Control + Shift + Eject ou Control + Shift + Power.

⁵ Clara Finance, Clara Pedagogy et GEREMI sont des exemples de systèmes décentralisés. Pour ces systèmes, le directeur responsable du système donne l'autorisation d'accès au membre du personnel. La direction des STI accorde l'accès autorisé par le propriétaire de données.

⁶ Pendant cette période, l'expert en la matière (EM) désigné par le directeur responsable assumera cette responsabilité. Lorsque le système passe en phase d'exploitation, les STI assument cette responsabilité et valident tous les droits d'accès actuels et futurs avec le directeur responsable. Tout accès jugé inutile/non pertinent pour la fonction de l'utilisateur sera supprimé par les STI après approbation du propriétaire des données.

⁷ Voir l'annexe B pour le tableau des RAI.

- créer, désactiver, réactiver ou supprimer des comptes de réseau et de courrier électronique « utilisateur », à la demande du gestionnaire, du directeur des installations et des STI respectifs ou du département des services des ressources humaines;
- attribuer des droits aux dossiers standard du serveur ainsi qu'aux dossiers spécifiques demandés (par Octopus) par le superviseur immédiat en raison de leur fonction et approuvés par le propriétaire des données;
- informer l'employé et son superviseur immédiat de l'accès aux comptes lorsqu'il est accordé;
- valider et ajuster (avec l'approbation de la direction des STI) les droits d'accès tous les six mois au besoin.

Les superviseurs immédiats (gestionnaires et présidents)

Les gestionnaires ont la responsabilité de veiller à que leur personnel ait connaissance de la présente annexe. Les utilisateurs n'ont pas le droit de s'attribuer eux-mêmes des autorisations aux systèmes.

En outre, les superviseurs immédiats doivent utiliser le centre de services du Cégep John Abbott (Octopus) pour ce qui suit :

- demandes de création, de réactivation, de désactivation ou de suppression de codes d'accès pour leur personnel/collègues;
- demandes de modification des paramètres des comptes (désactivation des comptes, modification des mots de passe ou autres mesures temporaires) pour les congés de maladie, de maternité/paternité ou autres congés;
- l'autorisation d'accorder des droits d'accès aux dossiers du réseau départemental au besoin (y compris les réactivations après le retour au travail);
- donner l'autorisation d'accès aux systèmes de leur département (Clara Finance, Clara Pedagogy, Geremi, Octopus, etc.) sous leur responsabilité et pour lesquels ils reçoivent une demande;
- gestion des noms d'utilisateurs pour les systèmes départementaux sous leur responsabilité (Clara Finance, Clara Pedagogy, Geremi, Octopus, etc.);
- demander une autorisation lorsqu'un membre de leur personnel doit accéder à un système départemental sous leur responsabilité.

Les Services des ressources humaines (SRH)

- Les Services des ressources humaines informeront les STI et les autres services concernés par courrier électronique lorsqu'un employé est nouvellement embauché (c'est-à-dire qu'il a signé son contrat), change de service, est en congé prolongé ou n'est plus au service du Cégep.

Le RAI

- Le RAI autorise ou refuse l'accessibilité aux systèmes et aux données des actifs informationnels sous la responsabilité de ce service.
- Le RAI examine régulièrement les rapports d'accès générés par la direction des STI.

Utilisation des comptes du Cégep

Droits d'administrateur

Les droits d'administrateur ne sont généralement pas accordés aux utilisateurs pour leur ordinateur. Les droits d'administrateur, lorsqu'ils sont accordés, sont temporaires et doivent être justifiés par la nature du travail et approuvés par le directeur du programme et le directeur des études (personnel enseignant) ou le directeur (personnel de soutien et professionnels) et le gestionnaire/directeur des STI. Lorsque la nature du travail prend fin, les droits d'administrateur sont retirés à l'utilisateur.

Il convient de noter qu'en cas de problème de fonctionnement d'un ordinateur sur lequel des droits d'administrateur ont été accordés à l'utilisateur, les STI ne feront aucune démarche pour récupérer les données de cet ordinateur. Le disque dur sera reformaté, ce qui entraînera la perte de toutes les données sauvegardées uniquement sur le disque dur de l'ordinateur.

Au Cégep

Les utilisateurs ne peuvent utiliser leur poste de travail que pour des activités liées au travail du Cégep.

En dehors du Cégep

Accès à distance par Office 365

Les utilisateurs ont accès à leur compte de messagerie, à leur calendrier et à d'autres services (One Drive, Share Point, MS Office en ligne, etc.) par le service Office 365.

Accès à distance par le portail

D'autres services tels qu'Omnivox, MIO, etc. sont disponibles par le portail du Cégep (Portail My JAC). Pour accéder à ces services, l'utilisateur doit disposer d'un compte Active Directory créé dès qu'un nouvel employé signe son contrat.

Les utilisateurs peuvent accéder aux éléments suivants par le portail @ <https://johnabbott.omnivox.ca>:

- compte de messagerie et boîte aux lettres MIO
- fichiers serveur limités grâce au service My Files
- configuration de la boîte vocale et messages téléphoniques
- module LEA Classroom
- d'autres modules Omnivox, y compris leurs fiches de paie, leurs reçus fiscaux, etc.

Accès à distance par un RPV (réseau privé virtuel)

L'accès RPV est une méthode sécurisée qui permet aux utilisateurs distants d'accéder aux mêmes fichiers que ceux dont ils disposent sur leur lieu de travail lorsqu'ils ne sont pas dans l'environnement du Cégep. Ce mode d'accès pose un problème général de sécurité, car les STI ne peuvent pas contrôler entièrement le poste de travail qui se connecte au réseau du Cégep; les utilisateurs doivent donc s'assurer qu'un programme antivirus actif est installé sur leur ordinateur et qu'il est mis à jour régulièrement. L'accès peut être refusé à tout ordinateur ne disposant pas d'un programme antivirus actif et mis à jour. Ce mode est réservé à des cas particuliers (administrateurs, techniciens des TI et autres utilisateurs autorisés).

Emploi

Employés nouvellement embauchés

- a. Après l'embauche, le directeur du SRH ou son délégué autorise la création du compte de l'employé par courrier électronique par Geremi (envoi automatique) à la direction des TSI avec les renseignements suivants :
 - i. le nom de l'employé
 - ii. le numéro d'employé
 - iii. le service ou le département de l'employé
- b. Après l'embauche, le SRH veille également à ce que l'employé reçoive le lien vers le site SharePoint « How-to » des STI, qui fournit des renseignements sur les points suivants et bien d'autres encore :
 - i. le compte informatique
 - ii. Office 365
 - iii. Mon portail JAC
 - iv. Octopus
 - v. les autres éléments pouvant être demandés par le logiciel du centre de service (Octopus) au besoin

En rapport avec les STI :

 1. la ligne téléphonique,
 2. CLARA Pedagogy (approbation du propriétaire des données requise),
 3. CLARA Finance (approbation du propriétaire des données requise),
 4. l'ordinateur (s'il n'y en a pas),
 5. l'accès aux dossiers de fichiers (approbation du propriétaire des données requise),

En rapport avec les SGD :

6. les clés (approbation de la direction ou de la direction adjointe7.6 requise),
7. le mobilier (si nécessaire).

c. Les STI créent les comptes du Cégep conformément aux renseignements fournis dans le courrier électronique du « nouvel employé » :

- i. Compte Active Directory
- ii. Inscription dans le répertoire téléphonique

- Pour les employés temporaires, une date de fin doit être présente pour que le processus soit achevé.
- Les STI peuvent communiquer avec le superviseur immédiat ou le directeur pour s'assurer que tous les renseignements et tous les droits sont pertinents.
- Les STI transmettent les codes d'accès et les mots de passe temporaires directement au nouvel employé qui, à son tour, a la responsabilité de changer son mot de passe lors de la première connexion.

Fin d'emploi (démission, retraite ou autre)

Lorsqu'un employé quitte le Cégep, volontairement ou non, le superviseur immédiat a la responsabilité d'informer le SRH et ce dernier doit ensuite informer les STI du dernier jour d'emploi au moins une semaine à l'avance. À la date de départ, les STI archiveront temporairement⁸ le contenu du dossier personnel et mettront en place un message de redirection sur le téléphone de l'employé vers un autre numéro choisi par le superviseur immédiat. Il convient de noter qu'en règle générale, les boîtes vocales ne sont pas conservées après le dernier jour de travail.

Par conséquent, avant la date de fin, le superviseur immédiat doit veiller à ce que

- tous les dossiers relatifs au département ou au service (documents, lettres, feuilles de calcul, bases de données, etc.) restent dans le dossier de l'employé jusqu'à ce que les STI reçoivent des instructions du superviseur de l'employé;
- il en va de même pour la boîte aux lettres électronique de l'employé;
- les retraités aient accès à leur boîte aux lettres électronique aussi longtemps que nécessaire, à condition qu'il y ait une activité continue sur le compte et qu'il soit financièrement possible pour le Cégep de le conserver;
- le poste téléphonique vers lequel les appels entrants de l'employé sortant doivent être redirigés soit déterminé (cela se produira pendant une période d'un mois, après quoi le transfert d'appels sera interrompu).

Mutations entre services ou départements

⁸ Les fichiers des utilisateurs sont archivés au moment du départ au cas où quelque chose aurait été oublié et devrait être récupéré. La suppression complète de toutes les données antérieures est effectuée conformément aux politiques de conservation des données du Cégep.

Lorsqu'un employé est muté d'un service ou département à un autre, le SRH a la responsabilité d'informer les STI du dernier jour de travail dans le service ou département sortant ainsi que du premier jour de travail dans le nouveau service ou département au moins une semaine à l'avance. (Pour les employés temporaires, une date de fin doit être précisée pour que le processus soit achevé.) Les STI se chargeront de supprimer les anciens accès et d'en accorder de nouveaux au besoin.

Par conséquent, une fois que la mutation vers le nouveau service ou département est approuvée, le directeur du SRH ou son délégué autorise la modification du compte de l'employé par courrier électronique à la direction des STI. Les STI enverront un message au superviseur/président de l'employé pour l'informer de l'arrivée du nouvel employé afin qu'il puisse demander d'autres articles à l'aide du logiciel du centre de services (Octopus), le cas échéant :

- i. une ligne téléphonique (si nécessaire)
- ii. CLARA pedagogy (si nécessaire),
- iii. CLARA finance (si nécessaire),
- iv. un ordinateur (s'il n'y en a pas),
- v. un accès au dossier des fichiers,
- vi. des clés (si nécessaire),
- vii. du mobilier (si nécessaire).

Avant la date de fin, le superviseur immédiat sortant doit veiller à ce que

- tous les dossiers relatifs au département ou au service (documents, lettres, feuilles de calcul, bases de données, etc.) soient transférés du dossier du personnel de l'employé à un dossier partagé du service ou du département;
- il en va de même pour la boîte aux lettres électronique de l'employé.

Il convient de noter que :

- les STI peuvent communiquer avec le superviseur immédiat ou le directeur entrant pour s'assurer que tous les renseignements et tous les droits sont pertinents;
- les STI transmettent les codes d'accès et les mots de passe temporaires directement au nouvel employé qui, à son tour, a la responsabilité de changer son mot de passe lors de la première connexion.

Annexe B

Système	Responsable des actifs informationnels (RAI)
Pédagogique	Directeur des systèmes académiques
Financier	Directeur des finances
Systèmes des RH	Directeur des Services des ressources humaines
Résidence	Directeur des Services aux étudiants
Casgrain	Directeur des Services aux étudiants
Dossiers départementaux	Chef du département