CHAMPLAIN
REGIONAL COLLEGE

DIRECTIVE SUR LES SERVICES EN LIGNE ET INFONUAGIQUES

Champlain
COLLEGE LENNOXVILLE

1958
St.Lawrence
CEGEP CHAMPLAIN

Champlain
COLLEGE SAINT-LAMBERT

Historique des révisions

Version	Date	Par	Type	Commentaires
0.1	4 octobre 2024	Claude Leduc	Création	
0,2	11 juin 2025	Claude Leduc	Modification	Révision et modification du contenu depuis la création
0.3	4 juillet 2025	Claude Leduc	Modification	Révision et modification du contenu depuis la création
0.4	12 septembre 2025	Claude Leduc	Modification	Révision du contenu à la suite de l'examen effectué par les coordonnateurs de la sécurité de l'information organisationnelle (COMSI)
0.5	6 octobre 2025	Claude Leduc	Modification	Révision du contenu à la suite du processus de consultation avec le comité de coordination informatique
0.6	27 octobre 2025	Claude Leduc	Modification	Modification apportée après le processus de révision par le comité de la haute direction (SMC)
1.0	18 novembre 2025	Claude Leduc	Approbation	Approuvé par le directeur général
1.01	21 janvier 2026	Claude Leduc	Correction	Réparation des liens défectueux

Table des matières

1. Préambule

Les services et applications basés sur l'infonuagique présentent des avantages considérables qui répondent aux besoins en constante évolution des établissements d'enseignement supérieur. Cependant, leur utilisation comporte des risques et est soumise à des réglementations, notamment en matière de protection et de sécurité des informations.

La « Directive sur les services en ligne et infonuagiques » (ci-après la « Directive ») du Collège régional Champlain (ci-après le « Collège ») vise à fournir des lignes directrices claires pour une utilisation responsable des services et applications infonuagiques, tout en garantissant la sécurité et la confidentialité des informations organisationnelles et personnelles, ainsi que leur conformité aux cadres réglementaires gouvernementaux ou organisationnels.

Avec l'évolution des technologies de l'information, les membres de la communauté du Collège stockent de nombreux documents organisationnels ou personnels sur diverses plateformes basées sur l'infonuagique. Le stockage de ces documents peut poser un défi sur les plans réglementaire et de la sécurité, car certains d'entre eux nécessitent un niveau de protection plus élevé en raison de leur sensibilité. Par conséquent, en complément de la politique de sécurité de l'information et de son cadre de gestion de la sécurité de l'information, la présente directive décrit l'utilisation appropriée des services et applications infonuagiques afin de renforcer la conformité, la sécurité et l'intégrité des informations organisationnelles tout au long de leur cycle de vie.

2. Objectifs

Les objectifs de la présente directive sont les suivants :

- Assurer la sécurité et la protection des informations, y compris les informations personnelles et les documents organisationnels sensibles ;
- Superviser la mise en œuvre des services et applications infonuagiques permettant au Collège de se conformer aux lois et réglementations en vigueur ;
- Détailler le processus d'autorisation d'accès et d'utilisation d'un service infonuagique ;
- Sensibiliser les utilisateurs aux différentes mesures de protection à appliquer aux informations stockées sur les plateformes infonuagiques ;
- Élaborer des principes directeurs ;
- Définir le niveau de responsabilité de chacun.

3. Cadre juridique et réglementaire

La directive s'appuie sur les lois, règlements et normes suivants :

- Directive gouvernementale sur la sécurité de l'information
- Cadre gouvernemental de gestion de la sécurité de l'information
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1)

- Règlement sur les incidents de confidentialité (LRQ, chapitre A-2.1, r. 3.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03)
- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03, r. 1)
- A-2.1, r. 2 - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (LRQ, chapitre A-2.1, r 2)
- Cadre de gestion des risques et des incidents liés à la sécurité de l'information gouvernementale
- Pratiques gouvernementales en matière de sécurité de l'information
- Exigences du ministère de la Cybersécurité et du Numérique (MCN) et des Centres opérationnels de cyberdéfense (COCD)
- Tous les règlements, politiques et règlements du Collège

4. Champ d'application

La présente directive s'applique à tous les membres de la communauté du Collège qui utilisent des ressources, des services et des applications infonuagiques à des fins académiques, administratives ou personnelles. Elle englobe tous les types d'informations couvertes par les lois et règlements gouvernementaux, les politiques institutionnelles, ainsi que l'utilisation de tout fournisseur de services infonuagiques fourni par le Collège.

5. Définitions

Actifs informationnels : toute information numérique, tout document numérique, tout système d'information, toute documentation, tout équipement informatique, toute technologie de l'information, toute installation ou tout ensemble de ces éléments acquis ou créés par le Collège pour mener à bien sa mission.

La **classification de l'information** consiste à identifier et à catégoriser les informations en fonction de leur niveau de sensibilité, de leur valeur et de l'impact potentiel que leur accès non autorisé, leur divulgation, leur modification ou leur destruction pourrait avoir sur l'organisation. L'objectif est de garantir que l'information est protégée et traitée de manière appropriée, conformément à son niveau de classification, aux exigences légales et réglementaires ainsi qu'aux besoins de l'organisation.

Le **Collège** désigne l'ensemble du Champlain Regional College, y compris ses collèges constitutifs, qui dispensent un enseignement général et professionnel.

La **communauté du Collège** désigne l'ensemble des étudiants, des enseignants et des employés. Pour les besoins de la présente Directive, elle comprend également les sous-traitants et les prestataires de services tiers, les invités des étudiants et du personnel, les représentants syndicaux, les représentants des associations étudiantes, les bénévoles, les sponsors et les membres des organes de gouvernance du Collège.

Les **documents ou informations organisationnels** sont des documents rédigés ou reçus par le Collège, l'un de ses départements ou services, ou par un employé dans l'exercice de ses fonctions (par exemple, un rapport d'activité, un procès-verbal ou un dossier étudiant).

Certains d'entre eux sont confidentiels, voire hautement confidentiels, car ils contiennent :

- Des informations dont l'accès et l'utilisation sont réservés à certaines personnes ;
- Des éléments stratégiques ou des renseignements personnels dont la divulgation non autorisée pourrait causer un préjudice grave aux membres de la communauté du Collège, au Collège ou à ses partenaires.

Un document peut être considéré comme non organisationnel s'il n'a aucun lien avec la fonction de l'employé qui le détient ou avec la mission du Collège (par exemple, une recette ou une photo de voyage).

L'**évaluation de la conformité** est une analyse approfondie de l'infrastructure, des contrôles de sécurité et des pratiques opérationnelles d'un fournisseur de services infonuagiques, afin de déterminer si ces éléments répondent à des normes réglementaires, juridiques et industrielles spécifiques. Elle aide les organisations à s'assurer que l'environnement infonuagique et les informations qu'il traite sont correctement protégés et conformes aux exigences pertinentes.

L'**évaluation des contrats** permet d'examiner les protections et les conditions contractuelles, notamment en ce qui concerne la responsabilité organisationnelle et individuelle, les conditions financières, la garantie, la propriété intellectuelle, ainsi que d'autres points si nécessaire. Elle permet de vérifier que les obligations du fournisseur (et de ses éventuels sous-traitants) offrent des protections généralement acceptables pour le Collège concernant les points susmentionnés, et que le Collège peut à son tour remplir ses obligations (y compris envers tout tiers). L'évaluation du contrat, qui est nécessaire pour garantir la diligence raisonnable, est basée sur le niveau de risque associé à l'acquisition du service infonuagique. Elle peut aller d'un « examen de base » à un « examen de base et une évaluation des clauses informatiques » :

- Examen de base :
    - Un examen de base se concentre sur l'examen de certains domaines qui préoccupent le Collège dans les conditions générales, tels que, mais sans s'y limiter :
        - Propriété intellectuelle (PI)
        - Responsabilité
        - Conditions financières
        - Confidentialité
        - Renouvellement/résiliation
        - Clauses inhabituelles
- Examen de base et une évaluation des clauses informatiques :
    - Cet examen porte sur l'ensemble des éléments des conditions générales et des accords associés.

L'**évaluation des facteurs relatifs à la vie privée (EFVP)** est un processus conçu pour protéger les renseignements personnels et respecter la vie privée des personnes. Il s'agit d'une forme d'évaluation d'impact. C'est un processus évolutif qui doit être révisé tout au long d'un projet.

Il s'agit de prendre en compte, avant le début d'un projet et tout au long de sa durée, tous les facteurs ayant un impact positif ou négatif sur la vie privée des personnes. Ces facteurs comprennent le respect des lois et des principes, l'analyse des risques et la mise en place de stratégies d'atténuation.

L'**évaluation des risques** permet de vérifier la probabilité qu'une solution infonuagique ait un impact sur la confidentialité, l'intégrité et la disponibilité des informations. Il s'agit du processus d'identification des risques de sécurité et d'évaluation des menaces qu'ils représentent. Elle permet également d'évaluer la capacité à gérer une cyberattaque ou une violation de données (résilience de la sécurité). L'objectif est d'atténuer les risques afin de prévenir les incidents de sécurité et les manquements à la conformité. Nécessaire pour garantir la diligence raisonnable, l'évaluation des risques est basée sur le niveau de risque associé à l'acquisition du service infonuagique. Elle peut aller d'une « évaluation limitée » à une « évaluation complète » du service infonuagique :

- Évaluation limitée :
    - L'examen des risques dans le cadre d'une évaluation limitée est effectué sur la base d'examens réalisés par des tiers. Les risques suivants sont examinés :
        - Risque de compromission des systèmes
        - Risque lié à la diligence
        - Risque lié au comportement des utilisateurs, tel que le partage de fichiers ou l'exposition des identifiants
        - Risque de divulgation publique
- Évaluation complète :
    - L'évaluation complète porte sur les points suivants :
        - Le fournisseur et ses produits/services concernés
        - Les tiers dont dépend le fournisseur
        - Les régions géographiques dans lesquelles le fournisseur héberge ses services ou peut accéder aux informations du Collège
        - Le schéma d'architecture de haut niveau de la solution complète du fournisseur
        - Le flux d'informations entre le Collège et le fournisseur, indiquant tout emplacement et tiers où les informations seront stockées
        - L'approche du fournisseur en matière de gestion des opérations informatiques, y compris la gestion des sauvegardes de données, la gestion des vulnérabilités techniques et la gestion des versions.

Gestionnaire : personne responsable de la sécurité d'un actif informationnel.

Incident : événement affectant ou pouvant affecter la disponibilité, l'intégrité ou la confidentialité des informations, ou plus généralement la sécurité des systèmes d'information, comme une interruption ou une dégradation des services.

Informations confidentielles : (voir l'annexe A) Il s'agit d'informations qui, si elles étaient divulguées sans autorisation, pourraient causer un préjudice à une personne, une organisation ou un gouvernement, mais pas nécessairement un préjudice grave ou irréparable.

Informations hautement confidentielles : (voir l'annexe A) Il s'agit d'informations qui, en raison de leur nature ou de leur contexte d'utilisation, sont susceptibles de faire l'objet d'une attente raisonnable en matière de confidentialité et pourraient causer un préjudice grave ou extrêmement grave si elles étaient compromises.

Informations institutionnelles : voir « Documents ou informations organisationnelles » Annexe A.

Les **informations organisationnelles réglementées** sont celles dont la protection est imposée par la loi, la réglementation ou les exigences du secteur.

> Il peut s'agir, par exemple, d'informations personnelles, de dossiers d'étudiants/employés, de mots de passe ou de dossiers juridiques.

Les **informations publiques sur l'organisation** sont des données qui ne sont pas confidentielles et pour lesquelles la protection n'est pas requise.

> Par exemple, un blog sur le site internet d'un collège.

Les **plateformes infonuagiques fournies par le Collège** sont approuvées pour le stockage et l'externalisation des informations. Elles sont régies par un contrat entre le Collège et le fournisseur de la plateforme et ont été déployées et intégrées à l'infrastructure informatique du Collège, à l'instar de la suite Office 365 et Microsoft 365.

Une **plateforme infonuagique publique** est une plateforme utilisée directement par l'utilisateur, qui n'est pas régie par un contrat entre le Collège et le fournisseur, et qui n'est pas déployée ni intégrée à l'infrastructure informatique du Collège. On peut citer, par exemple, OneDrive (version publique), Dropbox, iCloud, Evernote ou Google Drive.

Les **renseignements personnels** désignent tous les renseignements permettant d'identifier directement ou indirectement une personne, tels que le nom, l'adresse, le numéro de téléphone, l'adresse électronique, la profession, le numéro d'assurance sociale, la date de naissance, la photographie ou les renseignements bancaires. Ces renseignements doivent être protégés, quelle que soit leur forme (écrite, graphique, audio, visuelle, informatisée, etc.) ou leur support.

Renseignements personnels identifiables : voir « Renseignements personnels » et l'annexe A.

Renseignements protégés : voir « Renseignements personnels » et l'annexe A.

Les **services infonuagiques** sont des services ou des solutions logicielles gratuits ou payants fournis par un fournisseur externe via Internet. Avec ces services, les informations personnelles et organisationnelles sont stockées, traitées et transmises « dans le nuage », c'est-à-dire en dehors de l'infrastructure du Collège. Le Champlain Regional College a l'obligation légale de protéger les informations personnelles et de sauvegarder les informations sensibles.

Solution infonuagique : voir « Services infonuagiques ».

Le **stockage infonuagique,** ou stockage « cloud », désigne un modèle de stockage de données dans lequel les informations numériques sont stockées sur des serveurs distants gérés par un fournisseur tiers, plutôt que sur des appareils locaux. Ce modèle permet aux utilisateurs d'accéder à leurs données depuis n'importe quel endroit disposant d'une connexion Internet, éliminant ainsi le besoin de dispositifs de stockage physiques et simplifiant la gestion des données.

L'**utilisateur** désigne toute personne physique ou morale qui utilise ou a accès aux ressources d'information du Collège. Cette catégorie inclut, sans s'y limiter, les professeurs, le personnel professionnel, le personnel de soutien, les gestionnaires, les étudiants, les syndicats et associations qui les représentent, les locataires des logements étudiants et les fournisseurs de services tiers.

6. Principes directeurs

- **Confidentialité :** toutes les ressources informationnelles doivent être protégées contre tout accès ou toute divulgation non autorisés, qu'elles soient au repos ou en transit.
- **Intégrité :** les informations doivent être conservées de manière fiable et exacte, et protégées contre toute modification non autorisée.
- **Disponibilité :** les informations et les ressources doivent être accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin.
- **Conformité :** toutes les activités liées aux services cloud doivent être conformes aux lois, réglementations, obligations, règlements, politiques, cadres de gestion et directives institutionnels applicables.
- **Responsabilité :** tous les membres de la communauté du Collège sont responsables de leurs actions dans le cadre de l'utilisation des services infonuagiques.

7. Rôles et responsabilités

7.1. Chef de la sécurité de l'information organisationnelle (CSIO)

- Aide les responsables de l'information à analyser les risques liés à la sécurité de l'information ;
- Contribue au processus d'acquisition de biens et de services afin de s'assurer que les accords et contrats de service comprennent des dispositions visant à respecter les exigences en matière de sécurité de l'information ;
- Le CSIO, en collaboration avec le Comité de la haute direction (SMC), est responsable de la diffusion de la présente directive ;
- Le chef de la sécurité de l'information organisationnelle (CSIO) est chargé de mettre à jour la présente directive.

7.2. Équipe de sécurité de l'information (InfoSec)

- Soutient le chef de la sécurité de l'information organisationnelle (CSIO) dans l'application de la présente directive ;

- Évalue la conformité aux politiques, lois et règlements en vigueur en matière de gestion des risques liés à la sécurité de l'information.

7.3. Services des technologies de l'information

- Est chargé de l'application de la présente directive sur son site.

7.4. Gestionnaires

- Veillent à ce que leur équipe se conforme à la présente directive et aux politiques connexes lorsqu'elle utilise des services infonuagiques ;
- Facilitent les possibilités de formation et de développement afin d'améliorer la compréhension et la mise en œuvre de la présente directive par leur équipe ;
- Promeuvent une culture de responsabilité et de sensibilisation aux pratiques en matière de sécurité de l'information et de confidentialité parmi les membres de leur équipe.

7.5. Personnel et enseignants

- Veillent au respect de la présente directive et des politiques connexes lors de l'utilisation des services infonuagiques ;
- N'utilisent que des fournisseurs de services infonuagiques agréés et respectent les politiques institutionnelles en matière de classification et de protection des informations.

7.6. Étudiants

- Veillent au respect de la présente directive et des politiques connexes lors de l'utilisation de services infonuagiques ;
- Protègent leurs informations personnelles et celles d'autrui lorsqu'ils utilisent des services infonuagiques ;
- Utilisent les services infonuagiques de manière responsable.

8. Plateformes infonuagiques exploitées par le Collège

En ce qui concerne les services infonuagiques qu'il fournit, le Collège s'assure contractuellement que les fournisseurs incluent des clauses visant à protéger les informations stockées, conformément aux lois et règlements en vigueur.

Dans le cadre de sa stratégie opérationnelle en infonuagique, le Collège exploite une partie de son infrastructure sur la plateforme et les services Microsoft Azure. Le contrat de service prévoit que les centres d'hébergement des données soient situés au Québec et dans d'autres provinces canadiennes.

En tant qu'établissement d'enseignement, le Collège a également conclu un accord *Enrollment for Education Solutions (EES)* avec *Microsoft Canada Education* pour la suite, la plateforme et les services infonuagiques Microsoft 365. Les différentes applications et services sont principalement hébergés au Canada, mais certains sont encore exploités à l'extérieur du pays. Une liste détaillée est fournie en annexe de la présente Directive à titre de référence.

Dans le cadre de sa stratégie opérationnelle en infonuagique, le Collège utilise également une partie de son infrastructure auxiliaire sur la plateforme et les services Oracle OCI. Le contrat de service prévoit que les centres d'hébergement des données soient situés au Québec et dans d'autres provinces canadiennes.

Tous les contrats de services infonuagiques du Collège garantissent un niveau de protection des renseignements personnels équivalent à celui exigé par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1).

Le Collège fournit à chaque membre de la communauté collégiale un espace de stockage personnel (OneDrive for Business) ainsi qu'un accès facultatif à des espaces partagés (Teams/SharePoint). Ces espaces font partie de la suite Microsoft 365 et sont donc protégés par les conditions générales du contrat EES, telles que décrites ci-dessus.

Le Collège utilise également de nombreux autres services et applications infonuagiques. Ces services font partie du portefeuille d'applications administratives ou académiques. Ces autres services infonuagiques ne sont pas spécifiquement mentionnés dans la présente Directive. Toutefois, ils sont implicitement inclus dans l'application de la présente directive, dans le sens où aucune plateforme infonuagique ne peut être officiellement exploitée au sein du Collège sans validation et approbation préalables. Le processus d'autorisation est décrit dans le présent document.

9. Plateforme infonuagique publique

- Les employés ne peuvent pas stocker de documents contenant des informations protégées recueillies dans le cadre de leurs fonctions sur un service infonuagique public ou sur une plateforme qui n'est pas fournie et gérée par le Collège. Les services similaires, tels que Google Drive, iCloud, Dropbox et Evernote, ne peuvent pas être utilisés pour ce type de documents.

- Les employés ne peuvent stocker que des documents personnels non liés au travail sur des plateformes infonuagiques publiques.

- Le Collège n'a pas accès aux informations stockées sur les plateformes infonuagiques publiques et ne peut donc pas récupérer les données qui y sont stockées. Les employés qui utilisent ces plateformes doivent donc s'assurer qu'ils disposent de copies de sauvegarde des informations stockées sur ces plateformes, en cas de corruption ou de perte accidentelle.

- Afin de garantir la protection des informations personnelles, tous les utilisateurs qui ne sont pas des employés du Collège doivent respecter strictement les règles énoncées ci-dessus. Tout document contenant des informations personnelles sur d'autres personnes doit être exclusivement stocké sur une plateforme infonuagique fournie et gérée par le Collège.

10. Stockage infonuagique des informations organisationnelles

- L'espace de stockage et les normes de sécurité des informations sont déterminés par leur valeur, telle qu'établie par le système de classification des actifs informationnels du Collège, qui comporte trois niveaux de confidentialité : non confidentiel (public), confidentiel et hautement confidentiel.

- Bien que les utilisateurs puissent stocker des informations personnelles non liées au travail sur les plateformes infonuagiques fournies par le Collège, veuillez noter que ces informations ne pourront pas être conservées sur ces plateformes en cas de cessation d'emploi ou de fin d'études. Elles seront alors automatiquement détruites.

- Les informations hautement confidentielles ne peuvent être stockées dans une solution infonuagique que si elles ont fait l'objet d'une évaluation de sécurité par l'équipe chargée de la sécurité de l'information (InfoSec). Cette évaluation est nécessaire pour que la solution soit approuvée pour le stockage de ces informations et garantit qu'elles sont protégées de manière adéquate. En cas de changement de la solution, une nouvelle évaluation de sécurité par l'équipe InfoSec est nécessaire.

- Les informations hautement confidentielles transmises par courrier électronique doivent être protégées par cryptage.

- Aucune information personnelle, confidentielle ou hautement confidentielle ne doit être stockée dans une solution infonuagique dont les serveurs sont situés en dehors du Canada. Dans le cas contraire, une demande d'exemption doit être soumise à l'équipe chargée de la sécurité de l'information (InfoSec).

- L'équipe de sécurité de l'information (InfoSec) doit approuver toute solution infonuagique.

11. Teams/SharePoint

Les espaces de partage Teams/SharePoint peuvent être utilisés de manière facultative par les employés pour stocker des documents contenant des informations personnelles, organisationnelles ou confidentielles recueillies dans le cadre de leurs fonctions, sous réserve des règles de confidentialité spécifiques à chaque espace.

La version finale originale d'un document organisationnel doit être stockée dans l'espace de stockage utilisant la technologie désignée par le calendrier de conservation du Collège.

Les espaces de partage Teams/SharePoint peuvent être utilisés de manière facultative par les étudiants pour stocker des documents recueillis dans le cadre de leurs études. Cependant, ils doivent garder à l'esprit les règles décrites ci-dessus concernant le « stockage infonuagique des informations organisationnelles » en matière de conservation et de protection des informations.

Par défaut, les espaces Teams et SharePoint sont considérés comme « partagés ». Les utilisateurs doivent donc garder à l'esprit que les informations stockées dans ces espaces sont accessibles à d'autres personnes. Ils doivent également s'assurer que seules les personnes autorisées y ont accès.

Les espaces de partage Teams/SharePoint sont exclusivement réservés à l'hébergement de contenus en lien avec les activités éducatives et administratives. Tous les contenus doivent être conformes aux lois et réglementations en vigueur, notamment en matière de protection des droits d'auteur et de la propriété intellectuelle.

12. OneDrive

Le Collège fournit à chaque membre de sa communauté un espace de stockage « individuel » (OneDrive for Business).

L'espace de stockage individuel OneDrive vous permet de stocker et de gérer des documents et des fichiers à distance, depuis un ordinateur ou un appareil mobile, comme s'il s'agissait d'un serveur local.

Bien que cela ne soit pas recommandé, il est possible de stocker sur OneDrive des informations personnelles non liées au travail ou aux études.

OneDrive est mis à disposition en tant qu'espace de stockage individuel. N'oubliez pas que tout contenu doit respecter les lois et réglementations en vigueur, notamment celles relatives à la protection des droits d'auteur et de la propriété intellectuelle.

13. Appareils mobiles, partage et autres espaces de stockage

- Toute synchronisation d'informations institutionnelles hautement confidentielles ou confidentielles sur des appareils mobiles personnels, des ordinateurs portables ou tout autre espace de stockage est interdite.

- L'accès à tout appareil institutionnel ou personnel (par exemple, ordinateur de bureau, ordinateur portable, tablette ou smartphone) et son utilisation pour le traitement d'informations institutionnelles doivent être protégés par des mécanismes de sécurité, tels que le système de gestion des identités et des accès du collège, les codes d'accès (PIN), les empreintes digitales et la reconnaissance vocale, ainsi que d'autres bonnes pratiques en matière de sécurité de l'information.

14. Processus d'autorisation des services infonuagiques

Avant d'utiliser une solution infonuagique au sein du Collège (l'utilisation inclut le stockage, le traitement ou la transmission de données dans la solution), nous devons évaluer correctement cette solution afin de nous assurer qu'elle protège de manière adéquate les informations organisationnelles et personnelles. Une évaluation des facteurs relatifs à la vie privée (EFVP), une évaluation de la conformité, une évaluation des risques et une évaluation du contrat doivent être effectuées, quelle que soit la solution ou son coût.

Tous les services infonuagiques utilisés au sein de l'établissement doivent donc passer par un processus d'autorisation. Aucun service ne sera autorisé tant qu'il n'aura pas été validé et certifié. Si un service infonuagique est souscrit ou activé sans autorisation préalable, son utilisation sera immédiatement suspendue et l'abonnement résilié.

Il est donc essentiel de suivre ce processus de validation :

- Définir la solution infonuagique recherchée ; C'est à ce stade que les besoins sont définis et que la pertinence de l'utilisation du service infonuagique est établie.
- Réaliser un processus d'évaluation des facteurs relatifs à la vie privée (EFVP).
- Valider la conformité avec les lois, les réglementations et les obligations organisationnelles.
- Valider les exigences en matière de sécurité de l'information.
- Valider les conditions contractuelles.

Processus d'autorisation des services infonuagiques

	Demandeur	Responsabilités du réviseur
Évaluation initiale des besoins et examen	• Remplir le formulaire de demande de projet informatique et le soumettre aux services informatiques locaux pour un examen initial et une étude de faisabilité	Services informatiques locaux : • Examiner le formulaire soumis • Une fois examiné, soumettre le formulaire à InfoSec
Évaluation des facteurs relatifs à la vie privée (EFVP)	• Remplissez le formulaire d'analyse préliminaire EFVP	InfoSec : • Examinez le formulaire EFVP soumis • Soumettez le formulaire examiné au Comité de protection des renseignements personnels (CPRP)
Validation de la conformité		Services informatiques de l'unité administrative : • Examiner la conformité en fonction du contexte indiqué dans le formulaire d'acceptation du projet informatique

Évaluation des risques liés à la sécurité de l'information		InfoSec : Effectuer une évaluation des risques, allant de : • Aucune évaluation pour *les informations publiques* • Évaluation limitée pour toutes *les informations protégées* et *les informations réglementées de sensibilité faible/moyenne*, **À** • Évaluation complète pour *les informations réglementées de haute sensibilité*
Évaluation des contrats		Services informatiques de l'unité administrative et des achats : Effectuer une évaluation des contrats, allant de : • Examen de base pour *les informations publiques*, **À** • Examen de base et évaluation des clauses informatiques pour *les informations protégées et réglementées*
Décision : approbation, approbation sous conditions ou refus		

Lorsque vous envisagez de demander un accès à une solution infonuagique, vous devez tenir compte du fait que les évaluations requises prennent du temps. Elles impliquent en effet des échanges d'informations entre le fournisseur, ses sous-traitants, des auditeurs indépendants, le demandeur de la solution et plusieurs départements du Collège, afin d'évaluer la solution infonuagique demandée.

L'étendue de la diligence raisonnable requise dépend du niveau de risque associé à l'acquisition du service informatique. L'évaluation des risques nécessaire pour garantir cette diligence peut aller d'une évaluation « limitée » à une évaluation « complète » du service, et l'évaluation du contrat peut aller d'un « examen de base » à un « examen de base et évaluation des clauses informatiques ». Certaines exceptions peuvent toutefois s'appliquer.

Il sera obligatoire de documenter et de soumettre une demande d'autorisation préalable pour tout abonnement ou utilisation d'un service infonuagique. Cette demande doit être faite par écrit à l'équipe chargée de la sécurité de l'information et envoyée par courrier électronique à l'adresse suivante : infosec@crcmail.net .

14.1. Dérogations

Si une solution infonuagique n'a pas satisfait aux évaluations, une dérogation peut être accordée, au cas par cas et dans des circonstances exceptionnelles, pour l'utiliser dans des conditions spécifiques et pour une durée déterminée. Cette situation est rare et nécessite une autorisation écrite spéciale du responsable de la sécurité de l'information organisationnelle (CSIO) ou du directeur général du Collège.

14.2. Considérations

Lorsque vous utilisez un service infonuagique gratuit ou payant, vous devez vous poser les questions suivantes :

Quelles informations du Collège utiliserez-vous dans le nuage ?

> Lorsque vos informations sont stockées dans le nuage, le fournisseur de services infonuagiques y a généralement également accès. C'est pourquoi, en fonction du niveau de sensibilité des informations utilisées, il est nécessaire d'évaluer les solutions infonuagiques afin de s'assurer qu'elles offrent la protection requise par la législation québécoise et/ou canadienne.

Avez-vous vérifié que vous pouviez effectivement utiliser vos informations dans le nuage ?

> Vous devrez obtenir l'autorisation du responsable de l'information concernée, c'est-à-dire de la personne désignée comme responsable du type d'informations que vous souhaitez stocker dans le service infonuagique. Par exemple, si vous souhaitez utiliser des informations concernant les étudiants, l'autorisation du registraire sera nécessaire.

Quelles sont vos exigences ?

> Vos exigences doivent être complètes, claires, précises et cohérentes. Elles doivent identifier les informations qui seront stockées, traitées, transmises ou créées dans la solution infonuagique. Demandez-vous si vos informations sont considérées comme « publiques » ou « protégées ». Un processus d'évaluation des facteurs relatifs à la vie privée (EFVP) est requis. Ce formulaire vous demandera d'identifier clairement ces exigences. Il s'agit d'une étape du processus d'autorisation des services infonuagiques.

Avez-vous recherché d'autres solutions qui répondent à vos besoins ?

> Nous vous recommandons d'explorer plusieurs solutions, au cas où celle que vous demandez ne serait pas conforme aux obligations réglementaires auxquelles le Collège est soumis.

Dans combien de temps devez-vous commencer à utiliser le service infonuagique ?

> Tous les services infonuagiques, gratuits ou payants, doivent d'abord faire l'objet d'un processus d'évaluation afin de s'assurer que le Collège pourra se conformer aux lois et règlements applicables au Québec et au Canada en adoptant la solution d'un fournisseur. Ces évaluations impliquent des échanges d'informations entre le fournisseur et plusieurs services du Collège, afin d'évaluer sa capacité à protéger adéquatement les informations contenues dans sa solution.
>
> L'obtention et l'analyse de ces informations peuvent prendre jusqu'à trois mois, voire davantage. Vous devez donc tenir compte de ce délai lorsque vous planifiez l'acquisition d'une solution infonuagique.

Que se passe-t-il lorsque vous souhaitez renouveler le service infonuagique ?

Les services infonuagiques ne doivent pas nécessairement faire l'objet d'un processus d'évaluation lors du renouvellement, sauf si l'un des facteurs suivants est présent :

- Des problèmes ont été constatés concernant le niveau de service fourni par le fournisseur.
- Le fournisseur peut modifier ses processus, ses systèmes ou son « flux de données », ce qui peut avoir une incidence sur les hypothèses utilisées dans l'évaluation précédente.
- Toute violation du contrat liée à la sécurité, aux performances ou au respect de la confidentialité.
- Le champ d'application de la solution a changé ou va changer ; Cela peut impliquer des modifications des processus et/ou des informations associées (classification, volume, etc.).
- Des changements importants dans les lois et réglementations qui nécessiteraient une révision et éventuellement une modification du service.

15. Mesures transitoires

Toutes les informations institutionnelles contenant des données personnelles ou confidentielles, notamment des données hautement confidentielles, actuellement stockées dans une solution infonuagique non approuvée, doivent être transférées vers une solution institutionnelle approuvée. Les copies stockées dans des solutions infonuagiques non approuvées doivent être détruites.

16. Mise à jour de la présente directive

La présente directive fera l'objet d'une évaluation et d'une révision régulières, notamment en ce qui concerne la pertinence de ses dispositions par rapport aux nouveaux enjeux en matière de sécurité de l'information.

17. Date d'entrée en vigueur

La présente directive entre en vigueur à la date de son approbation par le directeur général et reste en vigueur jusqu'à ce qu'elle soit abrogée, modifiée ou remplacée par une autre directive.

Annexe A - TABLEAU RÉCAPITULATIF DES NIVEAUX DE CONFIDENTIALITÉ

INFORMATIONS NON CONFIDENTIELLES | FAIBLE RISQUE		
Définition	**Exemples**	**Risques potentiels**
• Informations non personnelles. • Informations qui n'ont aucune valeur stratégique pour le collège. • Les informations non confidentielles peuvent être divulguées librement, même si leur divulgation peut, dans certains cas, causer un préjudice minime.	• Les informations publiques comprennent notamment les informations publiées sur le site internet public du collège, les noms et coordonnées professionnelles du personnel enseignant et administratif du collège, le programme de la cérémonie de remise des diplômes, le guide des bourses, la convention collective en vigueur, le rapport annuel, le calendrier académique, la revue de presse, les supports de cours partagés en tant que ressources éducatives ouvertes, etc. • Les informations institutionnelles comprennent les statistiques, les listes et les inventaires ; les réglementations et les politiques en cours d'élaboration ou de révision ; les calendriers d'activités ; les documents liés aux affaires internes ; les descriptions de postes et de tâches ; les guides de formation ; les listes de cours ou d'événements par lieu ; un inventaire des actifs ; les modèles et formulaires ; les communications internes ; et les données de recherche non soumises à des restrictions légales ou contractuelles.	• Perturbations opérationnelles mineures

INFORMATIONS CONFIDENTIELLES | RISQUE MODÉRÉ		
Définition	**Exemples**	**Risques potentiels**
• Informations personnelles non sensibles. • Informations présentant une valeur stratégique modérée pour le collège. • Les informations confidentielles doivent être protégées contre tout accès, utilisation ou destruction non autorisés, conformément aux lois et réglementations en vigueur. La divulgation d'informations confidentielles à des personnes non autorisées pourrait causer un préjudice modéré au collège ou à des tiers.	• Informations concernant le dossier académique d'un étudiant, telles que les devoirs et examens effectués, les résultats scolaires, les relevés de notes et les dossiers étudiants qui ne contiennent pas d'informations sur la santé. • Informations identifiant des personnes sans informations personnelles sensibles, telles que les numéros d'identification des étudiants ou des employés, les coordonnées personnelles (adresse et numéro de téléphone), les listes d'inscription aux cours, les listes d'invités et les coordonnées pour les événements, ainsi que les documents de gestion du temps des employés (feuilles de temps, feuilles de présence et registres de présence). • Informations exclusives reçues d'un tiers dans le cadre d'un accord de non-divulgation. • Informations et dossiers financiers confidentiels.	• Préjudice modéré à l'encontre d'une ou plusieurs personnes ; impact modéré sur la réputation ou les activités du collège ; et perte financière modérée, telle que des amendes réglementaires.

INFORMATIONS HAUTEMENT CONFIDENTIELLES | RISQUE ÉLEVÉ		
Définition	**Exemples**	**Risques potentiels**
• Informations personnelles sensibles. • Informations présentant une grande valeur stratégique pour le collège. • Les informations hautement confidentielles doivent être protégées contre tout accès, utilisation ou destruction non autorisés, conformément aux lois et réglementations en vigueur. La divulgation de ces informations hautement confidentielles à des personnes non autorisées pourrait causer un préjudice grave au collège ou à des tiers.	• Les informations personnelles sensibles comprennent notamment les numéros d'assurance sociale, les dates de naissance, les données biométriques, l'origine ethnique, l'orientation sexuelle, les données de géolocalisation, les opinions des participants à des recherches, les numéros de permis de conduire, les numéros de passeport, les documents d'immigration, les dossiers d'admission, les dossiers des employés et les demandes d'honoraires professionnels contenant des numéros d'assurance sociale. • Les informations relatives à la santé physique et mentale d'une personne (ex. : le dossier médical, le dossier d'un étudiant, l'évaluation de son état de santé ou de sa condition physique, les documents relatifs à un congé de maternité). • Les informations sur la situation financière d'une personne (par exemple, étudiant, employé, participant à une recherche) : salaire des employés, demande d'aide financière, dossier des boursiers, informations sur les comptes bancaires et les cartes de paiement.	• Préjudice grave subi par une ou plusieurs personnes, usurpation d'identité, atteinte à la vie privée, impact grave sur la réputation ou les activités du collège, action en justice, perte financière importante, telle que des amendes réglementaires ou des dommages-intérêts résultant d'un litige.

	• Informations relatives à des enquêtes en cours, telles que des cas de plagiat, des litiges, des plaintes pour harcèlement, des affaires disciplinaires, des demandes de services juridiques, des griefs et des mesures disciplinaires.	

Annexe B – Résidence des données Microsoft 365

Produit	**Résidence des données**
Exchange Online	Canada
SharePoint (ODSP) et OneDrive	Canada
Microsoft Teams	Canada
Microsoft 365 Copilot	Canada
Office pour le Web (Office Online)	Canada
Microsoft Purview	Canada
Microsoft Entra ID	États-Unis
Whiteboard	Canada
Forms	Les données des formulaires sont stockées aux États-Unis. Les données des formulaires exportées vers Excel sont stockées au Canada.
Intune	États-Unis
Planner	Canada
Office pour mobile	Canada
OneNote	Canada
Power Apps pour Microsoft 365	Canada
Stream	Canada
Exchange Online Protection	Canada
Viva Connections	Canada