



Politique de sécurité

version 1.0, 21 avril 2023

- 1 – Introduction
- 2 – Définitions
- 3 – Champ d'application
- 4 – Mise en œuvre
- 5 – Rôles et responsabilités
- 6 – Politique
- 7 – Dispositions finales
- 8 – Historique des versions

1 – Introduction

Calcul Québec (« **CQ** ») gère et exploite des services de calcul informatique de pointe (« **CIP** ») pour soutenir l'excellence en recherche et en innovation au Québec et au Canada. En tant que fournisseur de services, Calcul Québec offre un ensemble diversifié de services, notamment des services de consultation et des services professionnels, l'infrastructure en tant que service (« **IaaS** »), la plateforme en tant que service (« **PaaS** ») et le logiciel en tant que service (« **SaaS** »). La présente politique concerne les mesures de sécurité nécessaires à la prestation de ces services.

Les politiques de Calcul Québec s'appliquent à tous les services offerts par Calcul Québec, conformément au mandat confié à CQ par les universités membres. Ces services utilisent des systèmes d'information dont les universités McGill et Laval sont les principaux propriétaires. Ils s'inscrivent dans le cadre d'un partenariat national via l'Alliance de recherche numérique du Canada.

En tant que fournisseur de services, Calcul Québec a des obligations en matière de protection des actifs et des données, ce qui comprend la protection des renseignements personnels (« **RP** ») et des renseignements personnels sur la santé (« **RPS** »). Les législations suivantes et les règlements qui en découlent s'appliquent aux activités de CQ ou de ses membres au Québec notamment :

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- Loi sur la protection des renseignements personnels dans le secteur privé;
- Loi concernant le partage de certains renseignements de santé;
- Loi sur les services de santé et les services sociaux;
- Loi concernant le cadre juridique des technologies de l'information.

En tant qu'organisation située au Canada, Calcul Québec doit également se conformer aux lois fédérales canadiennes telles que la *Loi sur la protection des renseignements personnels et les documents électroniques* (souvent désignée sous l'acronyme anglais PIPEDA). Ces lois contiennent des dispositions qui exigent que Calcul Québec, les Utilisateurs de CQ et les Locataires de CQ prennent des mesures raisonnables pour s'assurer que les RP/RPS sont protégés contre le vol, la perte et l'utilisation ou la divulgation non autorisée, et pour s'assurer que les dossiers contenant des RP/RPS sont protégés contre la copie, la modification ou l'élimination non autorisée. Si nécessaire, et dans la mesure applicable aux services de CQ, CQ utilisera des mesures raisonnables pour se conformer aux exigences du *Règlement général sur la protection des données* (« **RGPD** ») de l'Europe.

Les Utilisateurs et Utilisatrices de CQ et les Locataires de CQ peuvent être soumis à d'autres exigences légales ou réglementaires qui existent dans leur province, état ou pays. Ils peuvent également être liés à des politiques commerciales ou institutionnelles spécifiques et à des obligations contractuelles qui limitent ou empêchent leur utilisation des services de Calcul Québec. Il est de la seule responsabilité de l'Utilisateur, de l'Utilisatrice ou du Locataire de CQ d'identifier et de se conformer à toutes les exigences supplémentaires auxquelles ils sont assujettis.

Les exigences en matière de sécurité et de confidentialité seront établies en fonction des services spécifiques utilisés par un Utilisateur, une Utilisatrice ou un Locataire de CQ et en fonction du niveau de sensibilité des données qui y sont transférées, traitées ou stockées. Les objectifs suivants seront atteints par la mise en place de contrôles de sécurité, tels que décrits dans les autres sections de la présente politique.

- **Disponibilité de l'Information et des Systèmes d'Information de CQ.** L'Information et les Systèmes d'Information de CQ doivent maintenir un niveau de disponibilité conforme à leur rôle opérationnel et être compatibles avec le service spécifique, tel que défini dans l'Accord de niveau de service et les Conditions d'utilisation. L'architecture et les opérations des Systèmes d'Information de CQ doivent être surveillées et protégées afin d'éviter ou de remédier à toute interruption de service accidentelle ou non planifiée.
- **Confidentialité de l'Information.** Les droits d'accès et d'utilisation sont limités aux personnes autorisées, pour des usages et une durée autorisés. L'architecture et les opérations des Systèmes d'Information de CQ doivent être surveillées pour protéger, prévenir ou remédier aux accès non autorisés ou la divulgation d'informations.

- **Intégrité de l'Information et des Systèmes d'Information.** Les Systèmes d'Information de CQ et l'Information utilisée, stockée ou transmise sur un Système d'Information doivent maintenir un niveau d'intégrité conforme à leur rôle et être compatible avec le niveau de service, tel que défini dans l'Accord de niveau de service et les Conditions d'utilisation. L'architecture et le fonctionnement des Systèmes d'Information de CQ doivent être surveillés pour protéger, prévenir ou remédier aux dommages accidentels ou malveillants.
- **Accès à l'Information et aux Systèmes d'Information.** L'accès à l'Information et aux Systèmes d'Information doit être sécurisé et flexible, tout en assurant la confidentialité des données sans compromettre l'accessibilité légitime et la relative facilité d'utilisation.
- **Respect des exigences légales, réglementaires et contractuelles et des normes de diligence raisonnable.** Le respect de la législation applicable est continuellement évalué. De même, les risques liés à la sécurité ou à la confidentialité sont identifiés, évalués et gérés. Des mesures raisonnables sont prises pour détecter et prévenir les activités malveillantes. Les violations de la vie privée et les incidents de sécurité sont gérés conformément aux lois applicables et à l'Accord de niveau de service et les Conditions d'utilisation.

2 – Définitions

Les termes relatifs à la sécurité de l'information sont définis ci-dessous et disponibles dans le Glossaire de la sécurité de l'information¹ de CQ :

- **Accès privilégié** : un type d'accès qui accorde à une personne la permission d'effectuer une action qui est normalement non autorisée ou restreinte et qui accorde un contrôle supplémentaire sur l'Information ou un Système d'Information de CQ.
- **Accord de niveau de service** : accord par lequel le fournisseur de services (CQ) et un Utilisateur ou un Locataire de CQ s'engagent à respecter des conditions relatives au niveau de service offert par CQ. Il comprend, sans s'y limiter, le niveau attendu de disponibilité du service, l'attribution des responsabilités, les conditions d'accès et les conditions d'utilisation supplémentaires spécifiques au service.
- **Cadre de sécurité de l'information de CQ** : désigne un ensemble de politiques, de normes, de lignes directrices et de bonnes pratiques utilisées par Calcul Québec pour assurer la sécurité de l'Information et des Systèmes d'Information de CQ.
- **Conditions d'utilisation** : accord par lequel le fournisseur de service (CQ) et un Utilisateur ou un Locataire de CQ établissent les droits et obligations relatifs à l'offre de service globale de Calcul Québec.
- **Infrastructure as a Service (IaaS)** : services qui fournissent aux Locataires de CQ un ensemble de ressources dédiées qui relèvent uniquement de la responsabilité du

¹ <https://www.calculquebec.ca/glossaire-de-la-securite-de-information-CQ>

Locataire de CQ. IaaS s'apparente à un libre-service, où le Locataire de CQ est responsable de ses propres services, données, utilisateurs, système d'exploitation, configuration réseau, tout en tirant parti de l'infrastructure de CQ pour soutenir son environnement.

- **Information** : toute information ou donnée transmise, stockée ou traitée par un Système d'Information de CQ; ceci inclut, sans s'y limiter, les données de l'Utilisateur de CQ et les données du Locataire de CQ.
- **Information sensible** : Information classée comme Information de haut risque ou de très haut risque (voir la Directive sur la classification de la sécurité de l'information²).
- **Locataire³ de CQ** : un Utilisateur ou une Utilisatrice de CQ à qui ont été allouées des ressources IaaS. Ce faisant, le Locataire de CQ se voit accorder l'accès et la responsabilité exclusive de la gestion de ses ressources dédiées.
- **Membre de l'équipe CQ** : toute personne employée par, liée à ou travaillant pour le compte de Calcul Québec.
- **Platform as a Service (PaaS)** : services qui permettent aux Utilisateurs de CQ d'accéder aux informations et aux Systèmes d'Information de CQ d'une manière qui leur permet de gérer leurs propres logiciels et données. Les autres composants du système, tels que le système d'exploitation, l'infrastructure de stockage et la couche réseau sont gérés et exploités par CQ.
- **Renseignement personnel** : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- **Renseignement personnel sur la santé** : toute information sur une personne identifiable, vivante ou décédée, concernant sa santé physique ou mentale, ses soins de santé ou toute autre information liée à la santé concernant cette personne.
- **Sécurité de l'Information** : désigne les processus et méthodologies conçus et mis en œuvre pour protéger l'Information et les Systèmes d'Information de CQ contre tout accès non autorisé, utilisation abusive, divulgation, destruction, modification ou perturbation.
- **Software as a Service (SaaS)** : services qui permettent aux Utilisateurs de CQ d'accéder aux informations et aux Systèmes d'Information de CQ par le biais d'une interface logicielle qui leur permet de gérer leurs propres données. Les autres composants du système, tels que le système d'exploitation, les logiciels, l'infrastructure de stockage et la couche réseau sont gérés et exploités par CQ.

² <https://www.calculquebec.ca/directive-sur-la-classification-de-la-securite-de-information>

³ Le terme « Tenant » est généralement utilisé en anglais dans le contexte des services d'infonuagique.

- **Système d'Information de CQ** : tout système qui peut stocker, transmettre ou traiter des informations et qui est géré, exploité, régi ou réglementé par Calcul Québec.
- **Utilisateur / Utilisatrice de CQ** : désigne toute personne qui a accès à des Informations ou à un Système d'Information de CQ. Les personnes qui accèdent à des informations ou à des systèmes hébergés par un Locataire de CQ dans un environnement IaaS de CQ sont considérées comme des utilisateurs du Locataire de CQ et ne sont donc pas des Utilisateurs de CQ aux fins de la présente politique.

3 – Champ d'application

La présente politique s'applique à toute l'Information et à tous les Systèmes d'Information de CQ ainsi qu'à tous les Membres de l'équipe de CQ, aux Utilisateurs et Utilisatrices de CQ et aux Locataires de CQ. Les services ou l'Infrastructure du Locataire de CQ mis à la disposition des utilisateurs et utilisatrices du Locataire de CQ dans l'environnement IaaS sont hors du champ d'application de cette politique, car ils sont sous la responsabilité du Locataire de CQ et non de CQ elle-même.

4 – Mise en œuvre

La mise en œuvre et l'application des politiques de sécurité incombent à tous les Membres de l'équipe CQ, aux Utilisateurs et Utilisatrices de CQ ainsi qu'aux Locataires de CQ. Le non-respect de cette politique peut entraîner la révocation de l'accès de ceux-ci, ainsi que des mesures disciplinaires pour les Membres de l'équipe de CQ, tel que documenté dans le Cadre de sécurité de l'information de CQ. Le non-respect des lois applicables peut être considéré comme une infraction criminelle et être transmis aux autorités compétentes pour qu'elles prennent les mesures nécessaires.

La conformité au Cadre de sécurité de l'information de CQ est obligatoire. En cas de conflit perçu ou apparent entre les politiques de Calcul Québec, les Membres de l'équipe de CQ, les Utilisateurs de CQ et les Locataires de CQ doivent communiquer avec Calcul Québec, tel que décrit dans les Conditions d'utilisation ou l'Accord de niveau de service, pour une résolution immédiate.

Des vérifications ou évaluations indépendantes internes ou externes périodiques doivent être entreprises pour examiner ou évaluer la pertinence et l'efficacité des contrôles de sécurité mis en œuvre, y compris la conformité à la présente politique. Le RSI est responsable de l'examen périodique du Cadre de sécurité de l'information de CQ, au moins une fois par an, afin d'assurer son efficacité, son exactitude et sa conformité.

5 – Rôles et responsabilités

Direction générale de CQ : Relevant du conseil d'administration de CQ, est responsable de l'établissement des objectifs organisationnels en matière de sécurité de l'information et de l'allocation des ressources pour permettre et soutenir les fonctions de sécurité de l'information requises. La Direction générale de CQ est également responsable de l'approbation et de l'adoption des politiques requises afin de supporter la présente politique ainsi que de l'octroi d'exceptions à celles-ci le cas échéant.

Responsable de la sécurité de l'information de CQ (RSI) : Membre de l'équipe CQ sénior qui supervise le Cadre de sécurité de l'information de CQ. Le RSI fait partie de la direction de CQ et est responsable de :

- Développer et mettre en œuvre le Cadre de sécurité de l'information de Calcul Québec.
- Évaluer les risques liés à la protection de la vie privée et à la sécurité et être responsable de la protection des renseignements personnels dont CQ a la responsabilité.
- Évaluer les mesures et les contrôles de sécurité existants (p. ex., les procédures et les technologies permettant de vérifier l'identité des personnes auxquelles des droits d'accès doivent être accordés, la pseudonymisation ou l'anonymisation lorsque cela est possible, les mesures physiques visant à protéger l'infrastructure contre les risques naturels et les attaques, etc.) et rapporter sur leur efficacité.
- Se tenir au courant des nouvelles lois, réglementations, politiques, attentes et bonnes pratiques associées à la vie privée et à la sécurité et les partager avec les Membres de l'équipe CQ le cas échéant.
- Documenter et maintenir les politiques et procédures de sécurité de l'information et veiller à ce que les documents pertinents soient mis à la disposition des Utilisateurs, Utilisatrices et Locataires de CQ.
- Élaborer, mettre en œuvre et coordonner les programmes de formation et de sensibilisation à propos des mesures organisationnelles, physiques et techniques appropriées pour la protection de la vie privée et la sécurité de Calcul Québec et des services qu'il offre.
- Avoir une procédure en place, ou désigner une personne, pour recevoir et répondre aux déclarations de violations/incidents de données ou de sécurité provenant des Membres de l'équipe de CQ, des Utilisateurs et Utilisatrices de CQ ou des Locataires de CQ.
- Coordonner la réponse de Calcul Québec aux violations réelles ou suspectées, en ce qui concerne la confidentialité, l'intégrité et la disponibilité de l'information et des Systèmes d'Information de CQ.

Membres de l'équipe CQ : responsables de la protection de l'Information et des Systèmes d'Information de CQ en se conformant aux objectifs de confidentialité et de sécurité et aux exigences associées identifiés dans le Cadre de sécurité de l'information de CQ et dans la présente politique. Ces responsabilités comprennent :

- Exploiter, maintenir et soutenir les services de Calcul Québec et les Systèmes d'Information de CQ.
- Se tenir informé des politiques de sécurité, des exigences et des procédures opérationnelles en place à Calcul Québec.
- S'assurer que leur compte et leur appareil sont sécurisés.
- Se conformer aux mesures et contrôles de confidentialité et de sécurité approuvés par le RSI et inclus dans la présente politique et le Cadre de sécurité de l'information de CQ.
- Signaler au RSI (ou à la personne qu'il désigne) tout incident de sécurité ou toute atteinte à la vie privée, tel qu'identifié dans la présente politique et dans le Cadre de sécurité de l'information de CQ.
- Soutenir le RSI dans la réponse aux incidents en ce qui concerne la confidentialité, l'intégrité et la disponibilité de l'Information et des Systèmes d'Information de CQ et mettre en œuvre les actions nécessaires, conformément au mandat.

Utilisateurs / Utilisatrices de CQ : lors de l'utilisation ou de l'accès à l'Information ou aux Systèmes d'Information de CQ, ils et elles sont responsables de :

- Se conformer aux politiques de Calcul Québec ainsi qu'à toute autre politique pouvant être applicable à leur utilisation ou accès aux services de CQ.
- S'assurer que leur compte et leur appareil sont sécurisés.
- Signaler à Calcul Québec toute faille de sécurité, tout incident ou toute atteinte à la vie privée, tel qu'identifié dans le Cadre de sécurité de l'information de CQ.

Locataires de CQ : lors de l'utilisation de l'environnement IaaS de CQ, ils et elles sont responsables de :

- Se conformer aux politiques de Calcul Québec ainsi qu'à toute autre politique pouvant s'appliquer à leur utilisation ou à leur accès aux services de CQ.
- Surveiller et maintenir la confidentialité et la sécurité des services ou de l'infrastructure qu'ils hébergent dans l'environnement IaaS de CQ.
- Fournir à Calcul Québec un contact pour traiter ou signaler les événements de sécurité.
- S'assurer que leur compte et leur appareil sont sécurisés.
- Signaler à Calcul Québec toute vulnérabilité et/ou incident de sécurité ou toute violation de la vie privée, tel qu'identifié dans la présente politique ou dans le Cadre de sécurité de l'information de CQ.
- Gérer et accorder l'accès à leurs propres utilisateurs.
- Déployer et exploiter leurs propres services et infrastructures de manière sécurisée et être responsables de tout incident de sécurité ou de confidentialité dans ce contexte.
- Adopter des politiques, des normes et des processus adéquats pour garantir l'existence de mesures de protection appropriées dans leur domaine de responsabilité.
- Avoir une procédure en place avec leurs propres utilisateurs et utilisatrices pour recevoir et répondre aux incidents sur la vie privée et la sécurité et les signaler à CQ le cas échéant.

6 – Politique

1. Toutes les Informations et tous les Systèmes d'Information de CQ doivent être protégés d'une manière considérée comme raisonnable et appropriée à leur cycle de vie et à leur sensibilité, tel qu'approuvé par la direction de CQ et conformément au Cadre de sécurité de l'information de CQ. Ce cadre de sécurité de l'information, basé sur une approche de gestion des risques, vise à comprendre les risques existants ainsi que les stratégies et contrôles mis en place pour leur traitement.
2. Le Cadre de sécurité de l'information de CQ définira les modalités et restrictions d'accès aux Informations et Systèmes d'Information de CQ. Les accès doivent se limiter aux services ou Systèmes d'Information autorisés. L'accès à l'information sera restreint en fonction du principe du « besoin de savoir ». L'accès ou l'utilisation de l'Information ou des Systèmes d'Information de CQ doit être faite de manière vérifiable et auditable.
3. Les Membres de l'équipe CQ doivent recevoir périodiquement des formations ou sessions de sensibilisation relatives à la sécurité de l'information ainsi qu'aux politiques et normes de sécurité en vigueur à CQ. L'accès aux Informations sensibles nécessite une formation spécifique en matière de confidentialité et de sécurité.
4. En tant que fournisseur de services, Calcul Québec veillera à ce que les Locataires de CQ soient isolés les uns des autres afin d'assurer le maintien de la vie privée et de la confidentialité dans ses Systèmes d'Information. CQ s'assurera que le service et l'infrastructure qu'elle offre sont sécurisés et conformes à ses engagements, tels que définis dans l'Accord de niveau de service et Conditions d'utilisation applicables. Toutefois, la gestion des données, de l'infrastructure et des services hébergés dans un environnement IaaS de CQ relève de la seule responsabilité du Locataire de CQ. Cela inclut, sans s'y limiter, la gestion des accès et des droits des utilisateurs, les sauvegardes de l'environnement et de ses données, la maintenance et les mises à jour du système d'exploitation et des logiciels, la surveillance (sécurité et opérationnel) et la sécurisation des communications. L'accès privilégié des Membres de l'équipe de CQ aux services ou à l'infrastructure du Locataire de CQ hébergés dans un environnement IaaS n'est pas autorisé, sauf s'il existe une entente écrite à cet effet entre le Locataire de CQ et Calcul Québec.
5. Tous les Systèmes d'Information de CQ doivent être surveillés afin de détecter les intrusions et les utilisations ou accès non autorisés. La détection de tels événements par les Membres de l'équipe de CQ doit être signalée au RSI, et doit faire l'objet d'une enquête et de la mise en place de mesures d'atténuation appropriées pour empêcher toute exploitation ultérieure, tel que décrit dans le Cadre de sécurité de l'information de CQ. Tout problème de sécurité, abus ou accès non autorisé détecté par un ou une Locataire, un Utilisateur ou une Utilisatrice de CQ doit être signalé immédiatement à Calcul Québec⁴. Dans la situation où l'événement de sécurité est considéré par le RSI

⁴ Par courriel à securite@calculquebec.ca

comme ayant un impact sérieux sur les services ou l'infrastructure hébergés dans l'environnement IaaS, tous les Locataires de CQ affectés seront notifiés dans les plus brefs délais.

6. Dans le cas où un incident de sécurité est confirmé sur un Système d'Information de CQ, le RSI coordonnera immédiatement la réponse à l'événement avec les Membres de l'équipe de CQ chargés de mettre en œuvre les mesures pour rétablir, en temps utile, la confidentialité, l'intégrité et la disponibilité des Informations et des Systèmes d'Information de CQ. Pour les incidents où il y a également une violation de la vie privée ou un impact sur la sécurité des données, la réponse doit être conforme aux exigences identifiées dans la politique de confidentialité et de protection des données⁵. Les incidents de sécurité significatifs doivent être enregistrés et documentés conformément au Cadre de sécurité de l'information de CQ.
7. Les Systèmes d'Information de CQ seront maintenus à jour et supportés afin de minimiser l'exposition aux vulnérabilités de sécurité et de minimiser l'exposition aux risques, tel que décrit dans le Cadre de sécurité de l'information de CQ. Les changements apportés aux Systèmes d'Information de CQ doivent être gérés et autorisés uniquement par les Membres de l'équipe de CQ disposant de l'accès privilégié approprié, tel qu'identifié dans le Cadre de sécurité de l'information de CQ. Chaque changement mis en œuvre sera examiné afin d'évaluer et de minimiser son impact sur la confidentialité et la sécurité du Système d'Information de CQ avant sa mise en œuvre. Seuls les changements qui nécessitent une action de la part du Locataire, de l'Utilisateur ou de l'Utilisatrice de CQ ou ceux qui ont un impact sérieux sur le Système d'Information de CQ seront notifiés aux Locataires, Utilisateurs et Utilisatrices de CQ.
8. L'accès aux logs du Système d'Information de CQ est limité aux Membres de l'équipe CQ autorisés. L'Accord de niveau de service et les Conditions d'utilisation peuvent inclure des dispositions permettant à un Locataire de CQ d'accéder aux logs des Systèmes d'Information de CQ, à condition que la confidentialité et la vie privée des autres Utilisateurs, Utilisatrices et Locataires de CQ soient respectées.

7 – Dispositions finales

La politique entre en vigueur à sa date d'adoption. Toute question relative à cette politique ou à son interprétation peut être adressée à la Direction générale de CQ. Cette politique sera révisée au moins annuellement, afin de mieux répondre aux besoins de nos partenaires ou à de nouvelles exigences des gouvernements fédéral et provincial.

⁵ <https://www.calculquebec.ca/politique-de-confidentialite-et-de-protection-des-donnees>

8 – Historique des versions

Veillez vous référer au journal des modifications du document pour l'historique complet des versions de la présente politique. Les versions officielles précédentes peuvent être mises à disposition sur demande.