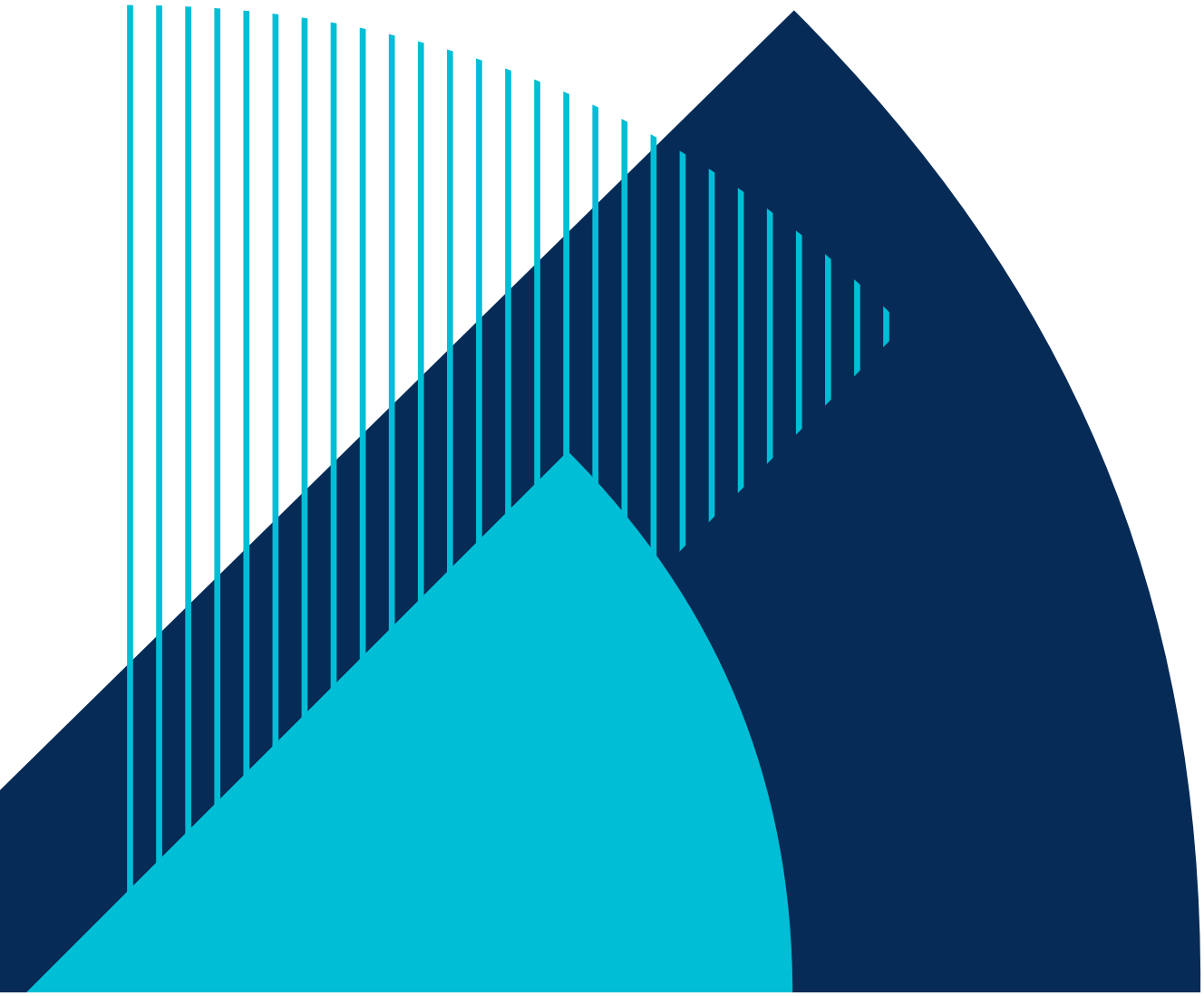
Politique de sécurité de l'information



INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Date d'approbation :	2025-01-30
Responsable de la mise à jour :	Chef de la sécurité de l'information organisationnelle (CSIO)
Dernière mise à jour :	Janvier 2025

Table des matières

1 Préambule

L'Institut de la statistique du Québec (ISQ) mise sur une culture de la confidentialité bien établie. Le respect de la vie privée et la préservation de la confidentialité des renseignements qu'il détient sont fondamentaux pour la survie de tout organisme statistique. Toute atteinte grave, réelle ou apparente, à la protection de l'information pourrait nuire à la confiance de la population ou des partenaires et avoir une incidence sur la notoriété de l'ISQ, sa capacité à réaliser sa mission et le respect de l'article 25 de sa loi constitutive.

Compte tenu de la nature hautement sensible de l'information traitée par l'ISQ, la protection de l'information revêt une importance capitale et doit faire l'objet d'un ensemble intégré de mesures qui s'inscrivent dans une structure de gouvernance bien définie. Ainsi, la sécurité de l'information doit être rigoureusement mise en œuvre dans chaque projet, qu'il soit de nature administrative ou statistique.

Cette politique de sécurité de l'information constitue la pierre d'assise de la gouvernance de l'ISQ en la matière et incarne sa vision. Elle décrit les objectifs, les principes directeurs, le champ d'application, les orientations ainsi que les rôles et les responsabilités des parties prenantes.

2 Définitions

Actif informationnel

Un actif informationnel peut être une information, quel que soit son support (papier, électronique, etc.) ou son canal de communication (téléphone, télécopie, voix, etc.), ou encore un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Authentification

Confirmation de l'identité d'une personne ou identification d'un document ou d'un dispositif.

Confidentialité

Propriété d'une information qui ne doit être divulguée qu'à des personnes ou à des entités désignées et autorisées.

Cycle de vie de l'information

Ensemble des étapes que franchit une information et qui comprend sa création, son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme public.

DIC, DICAI

Acronyme regroupant les trois propriétés fondamentales de l'information en matière de sécurité, soient la disponibilité, l'intégrité et la confidentialité (DIC), auquel peuvent être ajoutées l'authentification et l'irrévocabilité.

Disponibilité

Propriété d'une information qui est accessible en temps voulu et de la manière requise pour une personne autorisée.

Intégrité

Propriété d'une information qui n'a subi aucune altération ou destruction sans autorisation, et qui est conservée sur un support lui procurant stabilité et pérennité.

Irrévocabilité

Assurance qu'il est impossible de nier qu'une opération, un transfert ou une transaction a effectivement eu lieu. Également nommée « non répudiation ».

3 Cadre légal et administratif

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du Gouvernement*[1] (L.R.Q.,c. G-1.03) (LGGRI), adoptée en 2021, a notamment pour objet d'instaurer un cadre de gouvernance et de gestion en matière de ressources informationnelles applicable aux organismes publics et aux entreprises du gouvernement, d'assurer la protection adéquate des ressources informationnelles des organismes publics utilisées en soutien à la prestation des services publics ou à l'accomplissement des missions de l'État, d'accroître la résilience de l'administration publique et de rehausser la qualité et la protection de ces données.

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[2] a récemment été modifiée par une réforme législative, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[3], communément appelée « loi 25 ». L'envergure de la modernisation des lois en cette matière répond aux attentes de la population québécoise ainsi qu'aux défis posés par les avancées technologiques. Les modifications qui résultent de la loi 25 favorisent la transparence notamment des organismes publics, des entreprises et des partis politiques provinciaux, et donnent aux citoyennes et aux citoyens un meilleur contrôle sur leurs renseignements personnels. D'autres mesures assurent une meilleure protection de la vie privée de ces derniers, tout en tenant compte de la réalité technologique d'aujourd'hui. Des dispositions ont progressivement pris effet en septembre 2021, 2022 et 2023, et les dernières sont entrées en vigueur en 2024.

La *Loi sur l'Institut de la statistique du Québec*[4] a été révisée en 2021. Son article 25, qui va comme suit, concerne la sécurité de l'information : « Le statisticien en chef, les statisticiens en chef adjoints, les fonctionnaires et toute autre personne dont les services sont utilisés par le statisticien en chef dans l'exercice de ses fonctions ne peuvent révéler ni faire révéler, par quelque moyen que ce soit, des renseignements obtenus en vertu de la présente loi si ces révélations permettent de rattacher un renseignement à une personne, à une entreprise, à un organisme ou à une association en particulier. »

La Politique gouvernementale de cybersécurité[5], adoptée en mars 2020, vise à instituer une administration gouvernementale résiliente et cyberprotégée qui offre des services numériques centrés sur la personne. La mise en œuvre de cette politique se traduit par des mesures clés adaptées aux enjeux et aux possibilités en matière de cybersécurité.

La Politique s'applique à l'ensemble des organismes publics assujettis à la LGGRI. Elle concerne les relations de ces organisations avec les personnes qui utilisent les services publics et avec leurs partenaires, et établit les règles de gouvernance et de gestion en matière de ressources informationnelles.

1. www.legisquebec.gouv.qc.ca/fr/document/lc/G-1.03 (2021)
2. www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1
3. www.quebec.ca/gouvernement/ministeres-et-organismes/institutions-democratique-acces-information-laicite/acces-documents-protection-renseignements-personnels/pl64-modernisation-de-la-protection-des-renseignements-personnels
4. www.legisquebec.gouv.qc.ca/fr/document/lc/I-13.011
5. cdn-contenu.quebec.ca/cdn-contenu/gouvernement/SCT/vitrine_numeriQc/cybersecurite/politique-gouvernementale-cybersecurite.pdf

En plus des cinq principes fondamentaux sur lesquels la politique repose, le gouvernement s'est fixé neuf objectifs regroupés autour de quatre axes d'intervention afin, notamment, que la cybersécurité soit une priorité, que les services publics soient sécuritaires et que la population soit confiante et avertie.

La Politique gouvernementale de cybersécurité s'accompagne des documents suivants (certains remplacent ceux en vigueur, et d'autres sont présentement en révision) :

- La Directive gouvernementale sur la sécurité de l'information[6], en vigueur depuis le 8 décembre 2021, qui s'applique aux organismes publics visés à l'article 2 de la LGGRI. Elle a pour objet d'assurer une prise en charge adéquate et globale de la sécurité de l'information que les organismes publics détiennent ou utilisent dans l'exercice de leurs fonctions, même lorsque la conservation de l'information est assurée par un tiers. Elle remplace la Directive sur la sécurité de l'information gouvernementale, qui était en place depuis 2014.
- le processus de gestion des menaces, des vulnérabilités et des incidents (GMVI), publié le 22 juin 2022 par le Centre gouvernemental de cyberdéfense ;
- le Cadre gouvernemental de gestion de la sécurité de l'information[7], révisé sous l'Arrêté numéro 2022-04 du ministre de la Cybersécurité et du Numérique en date du 26 juillet 2022 ;
- le Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information[8], présentement en révision. À l'époque, ce document présentait une approche novatrice de détermination et de suivi du traitement des risques et des incidents susceptibles d'avoir des conséquences sur divers plans, dont la prestation de services à la population, la sécurité, la santé et le bien-être des personnes, la protection de leurs renseignements personnels ainsi que de leur vie privée, de même que des services fournis par d'autres organismes publics.

Ces documents déterminent les rôles et responsabilités des intervenants gouvernementaux et les obligations des organismes publics, notamment pour ce qui est d'adopter et de mettre en œuvre une politique de sécurité de l'information, la maintenir à jour et en assurer l'application.

Les autres lois et règlements qui régissent la présente politique sont présentés dans le document *Référentiel de la sécurité de l'information*.

6. SECRÉTARIAT DU CONSEIL DU TRÉSOR (2021), Directive gouvernementale sur la sécurité de l'information, [En ligne], Québec, 14 p. [www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/directive_securite_information2021.pdf].
7. GOUVERNEMENT DU QUÉBEC (2022), Gazette officielle du Québec, [En ligne], 154e année, no 24, Québec, Éditeur officiel du Québec, p. 3195-3200. [www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2022F/77425.pdf].
8. SECRÉTARIAT DU CONSEIL DU TRÉSOR (2014), Cadre de gestion des risques et des incidents à portée gouvernementale : Sécurité de l'information, [En ligne], Québec, 62 p. [www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_risques_incidents.pdf].

4 Objectif de la politique

La présente politique témoigne de l'engagement de l'ISQ de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit le support ou le moyen de communication.

Elle exprime la volonté ferme de l'ISQ de prendre en compte la sécurité de l'information dans le cadre de la réalisation de sa mission et de maintenir un haut niveau de confiance dans la population et auprès de ses partenaires.

Plus spécifiquement, les objectifs de l'ISQ en matière de sécurité de l'information sont les suivants :

- assurer, tout au long du cycle de vie de l'information, les différentes propriétés d'une information : disponibilité, intégrité, confidentialité, authentification et irrévocabilité (DICAI) ;
- atteindre un degré adéquat de sécurité de l'information par une compréhension commune et par l'engagement constant de tous les utilisateurs et utilisatrices, ainsi que des partenaires et fournisseurs ;
- adopter une gestion globale des risques, des menaces, des vulnérabilités et des incidents de sécurité de l'information pour l'ensemble des activités de l'ISQ ;
- soutenir la mise en œuvre de pratiques reconnues ;
- renforcer la responsabilité collective et individuelle en misant sur la diffusion d'information et sur des activités de sensibilisation en matière de sécurité de l'information.

5 Champ d'application

La présente politique s'applique à la sécurité de l'information sous toutes ses formes, qu'elle soit numérique ou non. Elle couvre plusieurs domaines d'intervention, dont celui des technologies de l'information, de la sécurité physique et de la gestion documentaire.

Elle s'adresse aux utilisateurs et utilisatrices, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui, à titre de membre du personnel, de consultante ou de consultant, de chercheuse ou de chercheur, de partenaire ou de fournisseur, utilise les actifs informationnels de l'ISQ ou y a accès ainsi qu'à toute personne dûment autorisée à y accéder.

L'information et les actifs informationnels visés sont ceux que l'ISQ détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Il s'agit, à titre d'exemple, de ceux :

- obtenus en vertu de la *Loi sur l'Institut de la statistique du Québec* ou d'un décret ;
- utilisés dans le cadre de la gestion des ressources humaines, matérielles et financières ;
- détenus ou confiés dans le cadre d'une entente contractuelle.

6 Principes généraux

L'atteinte des objectifs de la politique de sécurité de l'information s'appuie sur des principes applicables à tous. Toutes les parties prenantes sont imputables pour ce qui est du bon usage des informations dans le cadre de leurs fonctions. Les principes suivants guident les actions en la matière.

6.1 Gouvernance intégrée de la sécurité de l'information

La gouvernance de la sécurité de l'information repose sur une compréhension commune et sur une approche globale de la sécurité de l'information. Cette approche tient compte des aspects humains, organisationnels, juridiques et techniques et demande la mise en place d'un ensemble de mesures coordonnées visant à préserver adéquatement la confidentialité, et à garantir l'intégrité et la disponibilité de l'information.

6.2 Protection de l'information

L'information détenue par l'ISQ est essentielle à sa mission et doit faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate.

Le niveau de protection requis est établi en fonction de son importance, de sa confidentialité et des risques d'accident, d'erreur et de malveillance auxquels elle est exposée. Plus particulièrement, les mesures de sécurité visent les caractéristiques suivantes :

- assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées ;
- assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues ;
- limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance afin d'assurer une stricte confidentialité ;
- permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif via l'authentification ;
- assurer l'irrévocabilité, plus précisément prémunir l'Institut contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.

6.3 Responsabilité et imputabilité

L'efficacité des mesures de sécurité de l'information exige une attribution claire des responsabilités à tous les niveaux de l'organisation, y compris ses partenaires et les chercheuses et chercheurs, et la mise en place d'un processus de gestion interne de la sécurité comportant des mécanismes clairs d'imputabilité.

6.4 Droit de regard

L'Institut exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

6.5 Évolution et universalité des pratiques

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux ainsi que de l'évolution des menaces et des risques.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible et eut égard à la mission et au contexte des activités de l'ISQ, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

6.6 Éthique

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

7 Orientations

Les orientations guident l'élaboration des directives, processus, procédures, guides et autres actions pour concrétiser la mise en œuvre de la présente politique. Elles préconisent des actions prioritaires pour protéger les informations et les actifs informationnels jugés essentiels et stratégiques pour l'ISQ dans le contexte entre autres de la préparation au passage à l'infonuagique et de l'augmentation de la fréquence, la complexité et la virulence des cyberattaques. Pour les prochaines années, elles visent à :

- Renforcer la gouvernance de la sécurité en s'assurant :
  - de la disponibilité de l'information jugée essentielle et stratégique à la réalisation de la mission de façon à ce qu'elle soit accessible en temps voulu et de la manière requise et autorisée ;
  - de l'application à l'ISQ des mesures permettant de répondre aux exigences découlant du cadre légal et administratif s'appliquant aux organismes publics, minimalement de la réalisation d'audits de sécurité de l'information, de tests d'intrusion et de balayages de vulnérabilités à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information, et de proposer des actions conséquentes aux constats qui en découleront ;
  - que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires, ainsi que les chercheuses et chercheurs comportent des clauses garantissant le respect des exigences de sécurité de l'information.
- Formaliser des pratiques prévoyant la mise en œuvre de processus qui permettent d'assurer :
  - la gestion des risques de sécurité de l'information, qu'ils soient informatiques ou non, dès le début des projets, en s'appuyant sur une catégorisation officielle de l'information ;
  - la gestion des accès à l'information et la gestion des menaces, vulnérabilités et incidents (GMVI), ainsi que des événements de sécurité de l'information ;
  - l'organisation et la consignation des informations, des actions ainsi que des autres dimensions importantes de l'organisation concernant la sécurité de l'information à l'ISQ afin notamment d'assurer la compréhension commune des enjeux et des moyens mis en place pour y répondre.
- Collaborer avec des spécialistes de la protection des renseignements personnels (PRP) ainsi que des services juridiques, afin de s'assurer de la concordance des mesures permettant le respect des exigences en ce domaine.
- Développer et maintenir des compétences clés en la matière :
  - sensibiliser et former tous les utilisateurs et utilisatrices en fonction de leurs profils et des enjeux de sécurité de l'information.

8 Intervenantes et intervenants clés

Les intervenants clés s'engagent à soutenir les mesures et à mettre de l'avant les moyens nécessaires pour leur réalisation afin de minimiser les risques et d'assurer une gestion saine et intégrée de la sécurité de l'information au sein de l'ISQ.

- **La statisticienne ou le statisticien en chef** est la première ou le premier responsable de la protection et de la sécurité de l'information ainsi que de la gouvernance de ces aspects. Il ou elle nomme une cheffe ou un chef de la sécurité de l'information organisationnelle qui voit à la mise en œuvre de cette politique, nomme les membres du Comité stratégique de la sécurité de l'information, statue sur les avis et les recommandations, et désigne également les détenteurs et détentrices de l'information. Enfin, il ou elle approuve le plan d'action en matière de sécurité de l'information et autorise les budgets correspondants.
- **Le ou la chef de la sécurité de l'information organisationnelle** (CSIO) représente l'ISQ auprès de la dirigeante ou du dirigeant principal de l'information (DPI), qui est également chef gouvernemental de la sécurité de l'information (CGSI), et de la dirigeante ou du dirigeant de l'information (DI), qui est également chef délégué ou déléguée de la sécurité de l'information (CDSI). Il ou elle relaie également les orientations et les priorités d'intervention gouvernementales et de niveau portefeuille en ce qui concerne la sécurité de l'information. Il ou elle assiste la statisticienne ou le statisticien en chef dans la détermination des orientations stratégiques et des priorités d'intervention et le représente en ce qui a trait à la déclaration des risques et des incidents de sécurité de l'information à portée gouvernementale, assure la coordination et la cohérence des actions de sécurité de l'information menées à l'ISQ par les différentes parties prenantes et établit des partenariats internes à ces fins.
- **Le conseiller organisationnel ou la conseillère organisationnelle en sécurité de l'information** (COSI), en plus de son rôle de soutien auprès du CSIO, doit notamment aider les personnes détentrices à catégoriser l'information relevant de leur responsabilité et à analyser les risques pour la sécurité de l'information. De plus, il ou elle joue un rôle dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement en ce qui concerne l'identification, l'évaluation et la gestion des risques d'atteinte à la sécurité de l'information.
- **Le coordonnateur organisationnel ou la coordonnatrice organisationnelle des mesures de sécurité de l'information** (COMSI) et son ou sa substitut voient à la mise en œuvre du processus de la gestion des incidents de sécurité de l'information à l'ISQ, et font partie du réseau d'alerte gouvernemental.
- **Le ou la responsable de la protection des renseignements personnels** (RPRP) veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1). À ce titre, il ou elle doit communiquer au CSIO les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles, et assurer la cohérence et l'harmonisation des interventions avec la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale.

- **Le détenteur ou la détentrice de l'information, membre du personnel d'encadrement de l'ISQ**, a la responsabilité de veiller à la mise en place et à l'application des mesures de sécurité visant à assurer la protection de l'information qui est collectée, utilisée, communiquée, conservée ou détruite. Ces mesures doivent s'avérer raisonnables compte tenu, notamment, de la sensibilité, de la finalité de l'utilisation, de la quantité, de la répartition et du support de l'information. Le détenteur ou la détentrice de l'information a la responsabilité de catégoriser l'information relevant de sa responsabilité selon sa valeur en termes de disponibilité, d'intégrité et de la confidentialité.
- **Le ou la responsable de la gestion des technologies** (RGTI) a la responsabilité de mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique. Il ou elle s'assure de la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels lors de la réalisation d'un projet de développement ou lors de l'acquisition de technologies ou de ressources informationnelles.
- **Le ou la responsable de la sécurité physique** (RSP) met en place les mesures de protection physiques des actifs informationnels, des biens et des locaux.
- **Le ou la gestionnaire** est responsable, auprès du personnel relevant de son autorité et de toute personne à laquelle il ou elle accorde des accès à des actifs informationnels de l'ISQ de la mise en œuvre des dispositions de la présente politique et veille à ce que toutes et tous utilisent correctement les actifs informationnels. Il ou elle les sensibilise à la protection de l'information, aux conséquences d'une atteinte à la sécurité de l'information ainsi qu'à leurs responsabilités en la matière. Le ou la gestionnaire est responsable de la sensibilisation de son personnel et des personnes auxquelles il ou elle accorde des accès à des actifs informationnels de l'ISQ. Il ou elle voit également à inclure les clauses sur la sécurité et la protection de l'information dans les contrats et les ententes.

Les rôles et les responsabilités attribués, ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information, sont définis dans le *Cadre de gestion de la sécurité de l'information*, qui est en complément à la présente politique.

9 Obligations liées à l'utilisation

Toute personne qui utilise des données a l'obligation de protéger les informations et les actifs mis à sa disposition par l'ISQ. À cette fin, elle doit :

- prendre connaissance de la présente politique et y adhérer ;
- utiliser les actifs informationnels mis à sa disposition dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions en se limitant aux fins auxquelles ils sont destinés ;
- se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;
- signaler immédiatement au gestionnaire responsable tout acte dont elle a connaissance qui est susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des informations de l'ISQ ;
- respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger, et ne pas modifier leur configuration ou les désactiver. À cet effet, l'utilisateur ou l'utilisatrice confirme à l'ouverture d'un poste de travail de l'ISQ qu'il ou elle s'engage à respecter les modalités de la politique de sécurité de l'information et confirme comprendre que des sanctions peuvent être imposées en cas de manquement ;
- au moment de son départ de l'ISQ ou la fin de son mandat, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions. Les utilisateurs externes dont le mandat est terminé ou dont l'utilisation des informations de l'ISQ n'est plus nécessaire doivent demander le retrait de leurs accès.

10 Sanctions

Des vérifications et des enquêtes internes sont réalisées à la demande de la statisticienne ou du statisticien en chef pour vérifier le respect de la présente politique ou des directives en découlant. Toute personne qui y contrevient s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste, le tout suivant les conventions collectives, les autres conditions de travail de l'ISQ ainsi que les contrats et ententes en vigueur.

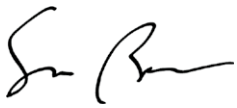
L'ISQ peut transmettre à toute autorité judiciaire les rengseignement colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

11 Dispositions finales

- La statisticienne ou le statisticien en chef approuve la présente politique.
- La ou le chef de la sécurité de l'information organisationnelle s'assure de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.
- La présente politique doit être actualisée à l'occasion de changements qui pourraient l'affecter.
- La présente politique sert d'assise au cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées dans des directives.

12 Entrée en vigueur

La politique de sécurité de l'information de l'ISQ est en vigueur dès l'approbation du statisticien ou de la statisticienne en chef.

2025-01-30	
Date approbation	Simon Bergeron, statisticien en chef

« Une organisation statistique performante au service d'une société québécoise en évolution »

statistique.quebec.ca

Institut de la statistique Québec