Règles de gouvernance concernant les renseignements désignés par le gouvernement et communiqués à des fins de recherche aux chercheurs liés à un organisme public

INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Pour tout renseignement concernant l'Institut de la statistique
du Québec (ISQ) et les données statistiques dont il dispose,
s'adresser à :

Institut de la statistique du Québec
200, chemin Sainte-Foy
Québec (Québec) G1R 5T4

Téléphone :
418 691-2401
1 800 463-4090 (Canada et États-Unis)

Site Web : statistique.quebec.ca

Ce document est disponible seulement en version électronique.

Dépôt légal
Bibliothèque et Archives nationales du Québec
4e trimestre 2023
ISBN 978-2-550-96065-2 (en ligne)

Octobre 2023

Avant-propos

Le présent document répond à une nouvelle exigence découlant de la modification de la *Loi sur l'Institut de la statistique de Québec* (LISQ), sanctionnée le 2 juin 2021. Conformément au nouvel article 30.3 de cette loi, l'Institut de la statistique du Québec (ci-après « l'Institut ») doit établir des règles pour encadrer la gouvernance à l'égard des renseignements désignés qu'il détient en vue de les communiquer aux chercheurs. Ces règles doivent notamment encadrer la protection, la conservation et la destruction de ces renseignements et prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements. Toujours selon cet article, la Commission d'accès à l'information doit approuver ces règles de gouvernance, qui seront ensuite publiées sur le site Web de l'Institut. Celles-ci devront être mises à jour et approuvées de nouveau par la Commission tous les trois ans.

C'est donc afin d'assurer le respect de ces exigences que l'Institut a produit une première édition de ces règles de gouvernance. Si l'application des nouvelles dispositions de la LISQ introduit assurément certaines nouveautés dans l'environnement réglementaire et fonctionnel des services d'accès aux données de recherche de l'Institut, bon nombre de pratiques et normes ici réunies sont en application depuis plusieurs années et témoignent bien de la longue expérience de l'Institut en matière d'exploitation de données administratives et de confidentialité des renseignements personnels. Le présent document fait état des différents contextes encadrant l'accès donné par l'Institut à des renseignements désignés pour la recherche et des moyens qu'il déploie pour répondre à ses engagements. Le document comporte les sept sections suivantes : 1) une mise en contexte ; 2) le cadre légal et institutionnel des nouvelles obligations de l'Institut ; 3) le cadre de gouvernance ; 4) les procédures et politiques en place ; 5) la reddition de comptes prévue ; 6) la présentation des renseignements désignés ; 7) les mesures déployées au fil du cycle de vie des renseignements.

Publication réalisée à
l'Institut de la statistique du Québec par : David Joubert-LeClerc, Jimmy Baulne, Linda Cazale, Marie-Claude Giguère et Patricia Caris

Avec la collaboration de : Assia Meloua-Benzaba, Sophie Balmayer, Luta Luse Basambombo, Fabienne Cléophat-Jolicoeur, Jocelyn Lefebvre, Isabelle Leroux, Stella Tiné et Maude Tremblay-Létourneau

Sous la direction de : Jimmy Baulne
Direction de la protection et de l'optimisation des données administratives

Patricia Caris
Secteur de la méthodologie et de l'accès aux données

Révision linguistique et édition : Direction de la diffusion et des communications

Pour tout renseignement concernant le contenu de cette publication : Institut de la statistique du Québec
200, chemin Sainte-Foy
Québec (Québec) G1R 5T4

Téléphone :
418 691-2401
1 800 463-4090 (Canada et États-Unis)

Site Web : statistique.quebec.ca

Notice bibliographique suggérée

INSTITUT DE LA STATISTIQUE DU QUÉBEC (2023). *Règles de gouvernance concernant les renseignements désignés par le gouvernement et communiqués à des fins de recherche aux chercheurs liés à un organisme public*, [En ligne], Québec, Institut de la statistique du Québec, 162 p.

Table des matières

1 Mise en contexte

À titre d'agence statistique de l'État québécois, l'Institut dispose de compétences méthodologiques et opérationnelles lui permettant de contribuer à offrir l'accès aux données d'enquête et aux données administratives à des fins de recherche. Depuis 1998, l'Institut est doté d'une loi constitutive garantissant le respect des mesures de protection des renseignements personnels (PRP) selon des standards reconnus par les organismes statistiques à travers le monde.

Dans les dernières années, le gouvernement a bonifié les moyens de l'Institut et a élargi ses mandats en matière d'accès aux données aux fins de recherche. Le point culminant est survenu en juin 2021, lorsque des modifications à la loi de l'Institut[1] sont venues accroître les capacités de l'organisme en matière d'accès aux données aux fins de recherche.

Dorénavant, l'Institut a également pour mission d'assurer la communication de renseignements détenus par des organismes publics et désignés par le gouvernement aux chercheurs liés à un organisme public à des fins de recherche.

Mesures annoncées dans les budgets du gouvernement depuis 2018

Depuis plusieurs années, le gouvernement bonifie les moyens de l'Institut et élargit ses mandats en matière d'accès aux données à des fins de recherche.

Au moment de la présentation du Plan économique du Québec en 2018, le gouvernement a annoncé l'implantation, par l'Institut, d'un guichet de services destinés aux chercheurs voulant obtenir, à des fins de recherche, des renseignements détenus par des ministères et organismes.

Le Plan économique du Québec 2019-2020 prévoyait quant à lui l'ajout des données provenant du ministère de l'Éducation, du ministère de l'Enseignement supérieur et de Revenu Québec, à celles du ministère de la Santé et des Services sociaux (MSSS) et à celles de la Régie de l'assurance maladie du Québec (RAMQ) déjà rendues disponibles.

Dans le budget rendu public en mars 2020, le gouvernement annonçait la mise en place de cinq nouveaux CADRISQ, des centres d'accès aux données de l'ISQ, notamment dans certains centres hospitaliers universitaires du Québec.

Dans le cadre du budget 2022-2023, le gouvernement a annoncé que les données du ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) ainsi que celles du ministère de l'Immigration, de la Francisation et de l'Intégration (MIFI) seraient ajoutées.

1. RLRQ, chapitre I-13.011.

2 Cadre légal et institutionnel

Loi sur l'Institut de la statistique du Québec[2]

La *Loi sur l'Institut de la statistique du Québec* (LISQ) a été modifiée à la suite de la sanction, le 2 juin 2021, de la *Loi concernant principalement la mise en œuvre de certaines dispositions sur le discours du budget du 10 mars 2020*[3]. Les changements apportés confèrent à l'organisation une mission élargie concernant l'accès aux données à des fins de recherche et précisent les conditions entourant la demande, la communication, l'utilisation et la destruction des renseignements désignés issus des organismes publics (chapitres I, I.1, I.2, III.1 et III.2).

Plus précisément, l'article 2.1 de la LISQ établit que l'Institut a dorénavant pour mission d'assurer la communication, à des fins de recherche, de renseignements détenus par des organismes publics aux chercheurs liés à un organisme public, conformément au chapitre I.2.

L'article 13.1 de la LISQ vient préciser que le gouvernement peut désigner des renseignements détenus par un organisme public afin qu'ils puissent être utilisés par l'Institut et communiqués à des fins de recherche à ces chercheurs liés à un organisme public.

De plus, l'article 30.3 vient notamment exiger que l'Institut établisse des règles encadrant sa gouvernance à l'égard des renseignements personnels désignés qu'il détient en vue de les communiquer aux chercheurs liés à un organisme public et les fasse approuver par la Commission d'accès à l'information (CAI). Ces règles, qui doivent encadrer la protection, la conservation et la destruction de ces renseignements, doivent également prévoir les rôles et les responsabilités des membres du personnel de l'Institut tout au long du cycle de vie de ces renseignements.

Par ailleurs, l'Institut accorde la plus haute importance à la confidentialité et à la protection de tous les renseignements qui lui sont confiées, que ceux-ci proviennent d'enquêtes ou de fichiers administratifs. Il en va de même pour les renseignements qui ont été désignés par le gouvernement. L'engagement de l'Institut à assurer la confidentialité découle de l'article 25 de sa loi, lequel prévoit que toute personne de l'Institut – qu'il s'agisse du statisticien en chef, des fonctionnaires ou de toute autre personne qui fournit des services au statisticien en chef – ne peut révéler ni faire révéler, par quelque moyen que ce soit, des renseignements obtenus en vertu de la loi si ces révélations permettent de rattacher un renseignement à une personne, à une entreprise, à un organisme ou à une association en particulier. Cette obligation s'applique aussi aux chercheurs admissibles qui ont accès à un fichier de recherche dans l'environnement contrôlé et sécurisé de l'Institut (CADRISQ ou en accès à distance).

2. RLRQ, chapitre I-13.011.
3. LQ 2021, chapitre 15.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[4]

L'Institut est aussi tenu de respecter la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès), récemment modifiée par la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels[5], qui impose notamment aux ministères et organismes de préserver la confidentialité des renseignements personnels permettant d'identifier des personnes.

4. RLRQ, chapitre A-2.1.
5. LQ 2021, chapitre 25.

3 Structure de gouvernance

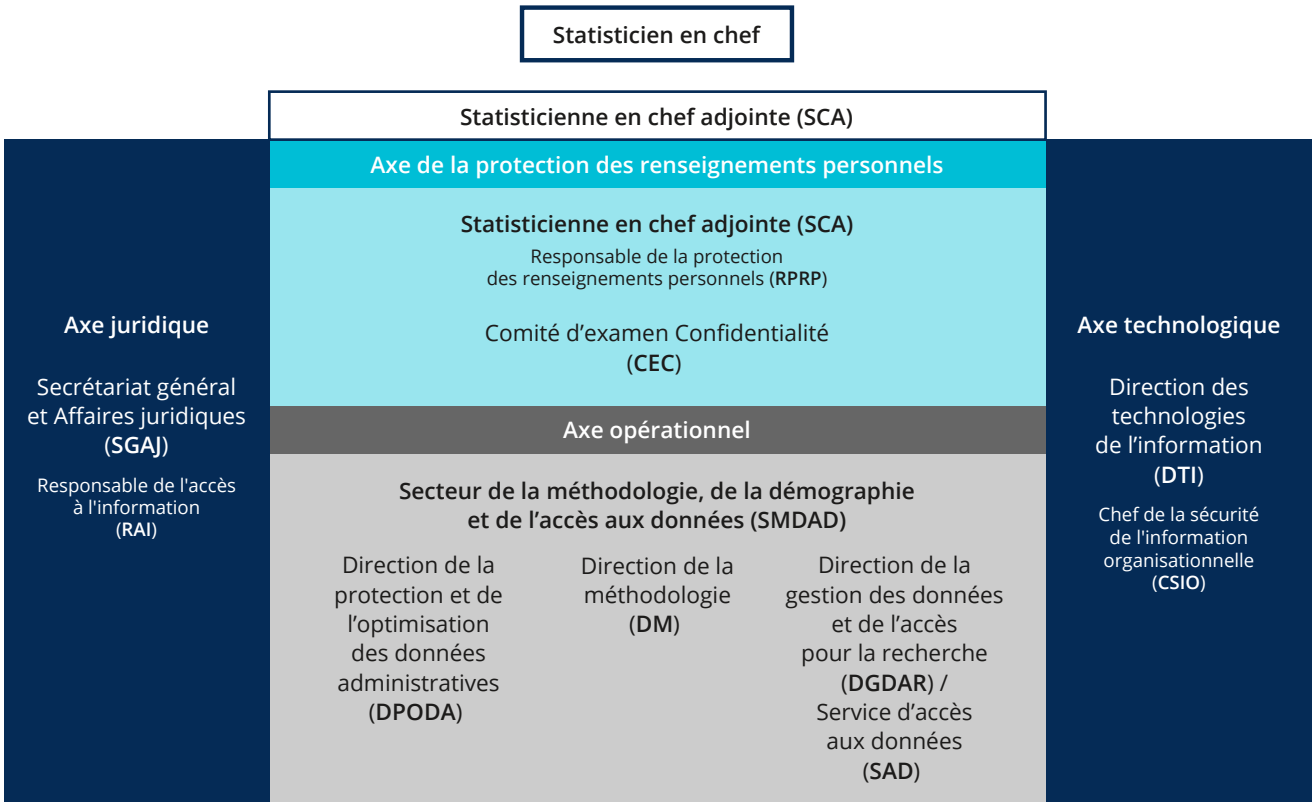
La structure de gouvernance de l'Institut concernant les renseignements désignés qu'il détient s'appuie sur des documents administratifs[6] qui établissent les devoirs et les conduites attendus des acteurs qui sont appelés à jouer un rôle dans le processus d'accès et d'utilisation des renseignements désignés dans le cadre de la recherche. Elle fournit un cadre pour que les meilleures pratiques soient en place et qu'elles soient revues en fonction de l'évolution du contexte afin de permettre l'accès aux renseignements désignés par les chercheurs admissibles, tout en assurant un équilibre entre la protection de ces renseignements et leur utilisation.

L'Institut tient compte des aspects humains, organisationnels, juridiques et techniques pertinents, et partage les rôles et les responsabilités entre les niveaux concernés de l'organisation. Sa gouvernance prend appui sur les lois et la réglementation en vigueur, dont la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement[7], qui établit les règles de gouvernance et de gestion à suivre en matière de ressources informationnelles.

6. Les documents administratifs peuvent notamment inclure des règlements, des politiques, des procédures, des directives et des modes opératoires normalisés.
7. RLRQ, chapitre G-1.03.

Rôles et responsabilités

Quatre axes viennent structurer les rôles et responsabilités concernant les renseignements désignés par le gouvernement et communiqués à des fins de recherche par l'Institut. L'axe de la protection des renseignements personnels et l'axe opérationnel de l'accès aux données ont un rôle prépondérant à jouer en matière d'accès aux renseignements désignés. Deux autres axes, soit l'axe juridique et l'axe technologique, sont transversaux et touchent donc l'ensemble des activités de l'Institut. Leur apport en matière de gouvernance est déterminant parce qu'adapté aux particularités d'une agence statistique.



Axe de la protection des renseignements

L'axe de la protection des renseignements se rapporte à la protection de tous les renseignements traités par l'Institut, qui incluent les renseignements personnels, mais ne se restreignent pas à ceux-ci. Cet axe est chapeauté par la responsable de la protection des renseignements personnels (**RPRP**), dont la fonction lui est conférée par le statisticien en chef en vertu de l'article 8 de la *Loi sur l'accès*. La RPRP a notamment pour responsabilité de produire les règles de gouvernance des renseignements désignés, et d'en assurer l'application et la mise à jour. Elle coordonne les efforts du personnel de l'Institut qui intervient dans les activités touchant les renseignements désignés pour la recherche. À ce titre, il lui incombe donc de gérer l'ensemble des activités liées aux renseignements désignés pour la recherche à l'Institut et de coordonner les efforts des quatre axes.

Soutenant directement la RPRP, le Comité d'examen Confidentialité (**CEC**) a pour rôle d'examiner les questions qui lui sont soumises en matière de confidentialité et de protection des renseignements personnels, et à rendre des décisions sous forme d'avis. Il est composé d'une dizaine de membres détenant des expertises précises en matière juridique, de confidentialité, de protection des renseignements personnels, d'éthique et de collecte de données. Il peut être interpellé pour tout enjeu de confidentialité en lien avec les activités de l'Institut. Depuis l'été 2017, il est aussi sollicité pour tout enjeu lié à l'accès aux données de recherche.

Axe opérationnel

L'axe opérationnel regroupe les unités qui offrent un service direct à la réalisation de la mission consistant à servir la recherche. Le Secteur de la méthodologie, de la démographie et de l'accès aux données (**SMDAD**) rassemble les acteurs opérationnels qui interviennent en première ligne dans le mécanisme d'accès aux renseignements désignés pour la recherche. Il s'assure d'une utilisation optimale des données administratives, tant aux fins de recherche que pour alimenter les demandes d'information de l'ensemble des ministères et organismes. Il regroupe :

- la Direction de la méthodologie (**DM**), dont le mandat général est de fournir expertise, assistance et conseil aux unités administratives de l'Institut, ainsi qu'aux ministères et organismes québécois, en méthodologie d'enquête, en utilisation de méthodes quantitatives, en analyse statistique des données et en analyse descriptive. Elle assure une veille des meilleures pratiques en méthodologie adoptées par les agences statistiques reconnues internationalement. Elle conçoit et applique des méthodologies d'enquête ou d'exploitation de fichiers administratifs, élabore l'infrastructure nécessaire au bon fonctionnement du système statistique, notamment en matière de confidentialité des données, évalue la possibilité de créer le fichier demandé, émet un avis quant à la possibilité d'accorder un accès à distance et, le cas échéant, détermine et applique le masquage nécessaire au fichier de microdonnées accessible à distance (FMAD) ;
- la Direction de la gestion des données et de l'accès pour la recherche (**DGADR**), qui gère, par l'entremise du Service d'accès aux données (**SAD**), la porte d'entrée unique des demandes d'accès aux renseignements désignés pour la recherche. Le SAD offre son expertise en matière d'analyse-conseil, de production de fichiers de recherche, d'exploitation des données, et de contrôle de la confidentialité des résultats. De plus, il est responsable des Centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ) ;
- la Direction de la protection et de l'optimisation des données administratives (**DPODA**), qui est responsable de l'analyse des demandes des chercheurs en matière de protection et de sécurité des renseignements et émet les recommandations à cet effet. Elle est également responsable des appariements nécessaires à la réalisation des projets de recherche. Elle maintient le lien avec les ministères et organismes pour les demandes d'accès aux renseignements désignés pour la recherche, et assure les liens entre les aspects légaux et administratifs et les services aux chercheurs. La direction doit également faire évoluer les différentes méthodes de protection des données et d'appariement.

Axe juridique

C'est essentiellement le Secrétariat général et Affaires juridiques (**SGAJ**) qui est chargé de l'axe juridique. Cette unité exerce un rôle majeur dans la gouvernance de l'Institut pour lui permettre d'agir comme coordonnateur statistique pour le Québec. À ce titre, le SGAJ contribue à une meilleure gouvernance, et propose des modifications au cadre administratif en tenant compte des enjeux organisationnels. Enfin, il assure le conseil juridique auprès de la RPRP, notamment par la coordination de l'ensemble des activités en lien avec l'application de la LISQ et de la *Loi sur l'accès*.

Axe technologique

La Direction des technologies de l'information (**DTI**) a pour mandat de soutenir les processus d'affaires de l'Institut relativement à la collecte, à la production, à l'exploitation et à la diffusion de données statistiques. À cet effet, elle assure les services-conseils ainsi que le développement, l'implantation et l'évolution des architectures, des outils, des systèmes d'information et des infrastructures technologiques dans le respect des normes et des orientations gouvernementales. Elle est également responsable de la sécurité applicative et opérationnelle qui vise à répondre aux exigences de la Politique de sécurité de l'information. Conformément à la *Directive gouvernementale sur la sécurité de l'information*,[8] la personne occupant la fonction de chef de la sécurité de l'information organisationnelle est responsable de l'établissement, de la mise en œuvre et de la révision des processus liés à la sécurité de l'information au sein de l'Institut.

Dans le cadre de l'accès aux renseignements désignés pour la recherche, la DTI s'occupe, entre autres, du maintien et du développement de l'infrastructure technologique des services d'accès aux données de recherche.

8. Secrétariat du Conseil du trésor [Québec] (2021), Québec, Direction des communications du ministère du Conseil exécutif, 14 p.

4 Politiques et procédures

Plusieurs politiques et procédures encadrant la réalisation de la mission et des mandats de l'Institut s'appliquent aux services d'accès aux données de recherche. La section qui suit décrit les mesures applicables à l'accès aux renseignements désignés par le gouvernement à des fins de recherche.

Politique d'accès aux microdonnées portant sur des individus ou des ménages

L'accès aux fichiers de microdonnées d'enquête ou aux fichiers de données administratives est encadré à l'Institut par la Politique d'accès aux microdonnées portant sur des individus ou des ménages. Cette politique précise les modalités d'accès disponibles selon le type de données demandées. Elle couvre notamment l'utilisation des renseignements désignés conformément à l'article 13.1 de la LISQ.

La politique prévoit qu'un chercheur lié à un organisme public puisse accéder à un fichier contenant des microdonnées détaillées dans un CADRISQ. Ce type de fichier comporte un potentiel analytique élevé puisqu'il est seulement dépersonnalisé, c'est-à-dire qu'il est exempt de renseignements identificatoires, mais qu'il contient toujours des identifiants indirects. En conséquence, des exigences légales et administratives ainsi que des mesures de sécurité physique et informatique sévères encadrent son utilisation et réduisent le risque de divulgation d'information confidentielle.

Cette politique contient également des informations quant aux mesures de protection appliquées à certains fichiers de microdonnées en vue de leur dépersonnalisation, de leur anonymisation ou simplement de la réduction du risque de divulgation d'information confidentielle. Il est important de souligner qu'avant tout traitement de données, l'Institut effectue une séparation entre les renseignements identificatoires et les autres renseignements nécessaires à la recherche.

Par ailleurs, des mesures de contrôle de la divulgation sont appliquées pour veiller à ce que l'engagement à la confidentialité des organismes statistiques soit respecté, tout en assurant autant que possible l'utilité des données produites. Certaines mesures spécifiques sont utilisées lors de la création des fichiers de microdonnées accessibles à distance (FMAD).

Politique relative à la confidentialité des tableaux de résultats pour diffusion

L'Institut effectue une vérification du risque de divulgation associé à tout résultat issu de données de recherche destiné à être diffusé, afin de contrôler adéquatement le risque de divulgation d'information confidentielle.

Une analyse de divulgation permet d'évaluer le risque de dévoiler une information confidentielle lors de la diffusion (sortie de l'environnement sécurisé de l'Institut) d'un résultat statistique (tableau, modèle, graphique, etc.). Lorsque le risque est trop élevé, des techniques de masquage doivent être appliquées afin de réduire ce risque et de permettre la diffusion du résultat.

Qu'il s'agisse de produits statistiques créés à partir de données administratives (renseignements désignés ou non désignés) ou de données d'enquêtes, les chercheurs, qu'ils y accèdent dans un CADRISQ ou à distance, doivent en tout temps respecter les règles de confidentialité de l'Institut. Ces règles, qui peuvent varier selon la nature des données traitées (données administratives ou données d'enquête), sont spécifiées dans la Politique relative à la confidentialité des tableaux de résultats pour diffusion.

Les résultats intermédiaires constituent des analyses préliminaires qui ne sont pas destinées à la diffusion et qui demeurent dans l'environnement sécurisé de l'Institut. Ils ne sont pas assujettis aux règles de confidentialité prévues pour la diffusion, étant donné qu'ils demeurent dans l'environnement sécurisé de l'Institut et qu'ils ne peuvent être accessibles qu'aux membres de l'équipe de recherche.

Politique de sécurité de l'information

La politique de sécurité de l'information de l'Institut définit les principes généraux de la gouvernance de la sécurité de l'information.

Elle s'adresse à tous les utilisateurs, c'est-à-dire à tout le personnel de l'Institut, peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels de l'Institut ou y a accès, ainsi qu'à toute personne dûment autorisée.

L'accès aux renseignements désignés est limité aux employés et aux chercheurs qui démontrent la nécessité d'y accéder et qui y sont dûment autorisés. L'Institut a élaboré des environnements sécurisés afin de faciliter le contrôle de l'accès à ces renseignements, et ce, tant pour les employés de l'Institut que pour les chercheurs autorisés. De plus, les accès à ces environnements sont journalisés afin d'en garantir la légitimité.

Des vérifications et des enquêtes internes sont réalisées à la demande du statisticien en chef pour assurer le respect de la politique et des directives en découlant. Si l'utilisateur y contrevient, il s'expose à des mesures disciplinaires, qui peuvent être administratives ou légales.

Politique de sécurisation des locaux

L'Institut dispose depuis 2003 d'une politique de sécurisation des locaux qui définit les rôles et responsabilités, le zonage, les mesures de contrôle et les modalités d'application relatives à la sécurité physique de ses locaux. Cette politique encadre notamment l'accès aux CADRISQ et aux serveurs contenant les renseignements désignés pour la recherche.

Cadre de gestion de la sécurité de l'information

Le cadre de gestion de la sécurité de l'information de l'Institut vient appuyer la mise en œuvre des dispositions de la Directive sur la sécurité de l'information gouvernementale. La directive prévoit que le dirigeant d'un organisme public, en prenant appui sur les orientations et les bonnes pratiques gouvernementales en matière de sécurité de l'information, doit adopter et mettre en œuvre une politique et un cadre de gestion de la sécurité de l'information, les maintenir à jour et assurer leur application.

Procédure de traitement des demandes d'accès aux données de recherche

Le chercheur admissible qui désire accéder aux renseignements désignés doit soumettre une demande d'accès sur le site Web des services d'accès aux données de recherche de l'Institut. Une évaluation standardisée est ensuite réalisée afin de statuer sur la recevabilité de la demande, sur la faisabilité technique et logistique, ainsi que sur le respect de critères propres aux aspects éthiques et juridiques, et à la protection des renseignements personnels. Une recommandation est ensuite formulée au responsable de la protection des renseignements personnels de l'Institut. La procédure décrit en détail les étapes d'analyse et d'approbation nécessaires pour obtenir l'accès à des renseignements désignés à des fins de recherche.

Processus de gestion et de traitement des incidents en sécurité de l'information

L'implantation d'un processus de gestion et de traitement des incidents en sécurité de l'information axé principalement sur la prévention et la détection des incidents ainsi que sur la réponse à ceux-ci est essentielle à l'Institut. Le but est d'atténuer les risques et de s'assurer qu'en cas d'incident en sécurité de l'information, les mesures appropriées seront prises, les personnes concernées seront contactées et, le cas échéant, les étapes nécessaires à la tenue d'une enquête seront réalisées correctement. Ce processus vise tout le personnel de l'Institut, peu importe son statut, toute personne physique ou morale qui agit à titre d'employé, de consultant, de partenaire ou de fournisseur, ainsi que toute personne témoin d'un incident de sécurité dans le cadre d'une prestation de travail.

5 Reddition de comptes

Afin de démontrer la saine gestion des renseignements désignés dont il est responsable, l'Institut doit rendre compte de l'utilisation de ceux-ci. La reddition de comptes prévue à l'égard des renseignements désignés vise à faire la démonstration que l'Institut s'acquitte adéquatement de ses responsabilités. Elle s'adresse à la Commission d'accès à l'information (CAI) et aux organismes publics détenteurs des renseignements désignés de même qu'aux citoyens selon les dispositions contenues dans la LISQ. De plus, dans un but de transparence, l'Institut publie ses règles de gouvernance sur la page Web des services d'accès aux données de recherche.

À la Commission d'accès à l'information (CAI)

Les règles de gouvernance des renseignements désignés pour la recherche sont un élément central du processus de reddition de comptes (LISQ, art. 30.3). Ces règles, d'abord approuvées par la CAI une première fois en 2022, devront être revues et approuvées selon un cycle de trois ans. L'Institut doit, sur demande de la CAI, lui fournir toute l'information qu'elle requiert à l'égard de leur application (LISQ, art 30.5).

L'Institut doit transmettre à la CAI :

- la copie de toute désignation de renseignements détenus par un organisme public, afin qu'ils puissent être utilisés par l'Institut et communiqués à des fins de recherche aux chercheurs liés à un organisme public (LISQ, art. 13.1) ;
- les copies de toute entente de communication liant l'Institut et un chercheur lié à un organisme public et ayant conclu une entente de communication au sujet d'une activité de recherche comprenant des renseignements désignés (art. 13.11), dans les 30 jours suivant sa conclusion.

Par ailleurs, conformément aux articles 13.4 et 13.16 de sa loi constitutive, l'Institut s'engage à publier sur son site Web une liste des renseignements désignés, rattachés à chaque organisme public qui les détient, de même qu'un registre des publications des résultats des recherches pour lesquelles des renseignements désignés ont été communiqués.

Soulignons que l'entente de communication conclue entre un chercheur et l'Institut prévoit que ce dernier et la CAI doivent être avisés sans délai par le chercheur du non-respect de toute condition prévue à l'entente, de tout manquement aux mesures de protection prévues à l'entente, ou de tout événement susceptible de porter atteinte à la confidentialité des renseignements (LISQ, art. 13.10, al. 4). Précisons que l'Institut a déjà mis en place un cadre de gestion des incidents de confidentialité général, avec notamment son Processus de gestion et de traitement des incidents en sécurité de l'information et sa Politique de sécurité de l'information.

Aux organismes publics détenteurs des renseignements désignés

La reddition de comptes aux organismes publics prévoit la transmission d'une copie des ententes prévues à l'article 13.9 de la LISQ établies entre l'Institut et un chercheur lié à un organisme public et conclues au sujet d'une activité de recherche se fondant sur des renseignements désignés, dans les 30 jours suivant sa conclusion (art. 13.11).

Lorsque l'Institut est avisé du non-respect de toute condition prévue à l'entente de communication conclue avec un chercheur, de tout manquement aux mesures de protection y étant prévues, ou de tout événement susceptible de porter atteinte à la confidentialité des renseignements, il doit en aviser sans délai l'organisme détenteur des renseignements concernés.

Aux citoyens

La reddition de comptes aux citoyens se fait sur le site Internet de l'Institut. La liste des renseignements désignés, rattachés à chaque organisme public qui les détient, y est publiée. De plus, l'Institut y affiche un registre des publications des résultats de recherche pour lesquelles des renseignements désignés ont été communiqués à des chercheurs.

6 Renseignements pour la recherche

Renseignements désignés

La LISQ prévoit que des renseignements détenus par un organisme public peuvent être désignés afin d'être transmis à l'Institut, lequel pourra les utiliser et les communiquer à des fins de recherche aux chercheurs liés à un organisme public (art. 13.1). Les renseignements sont désignés par le gouvernement sur recommandation conjointe du ministre des Finances et du ministre responsable de l'organisme public qui détient les renseignements (art. 13.2).

L'organisme public détenteur de ces renseignements doit, sur demande de l'Institut, lui communiquer les renseignements désignés qu'il détient selon des modalités convenues. La liste des renseignements désignés est tenue à jour par l'Institut, qui la rend disponible sur le site Web des services d'accès aux données de recherche de l'Institut, au statistique.quebec.ca/fr/institut/services-recherche/donnees.

Selon la volonté du gouvernement, de nouveaux renseignements peuvent être désignés. Le cas échéant, ces renseignements sont ajoutés à la liste des renseignements disponibles pour la recherche sur le site Web de l'Institut une fois l'ensemble des étapes de désignation réalisé.

Autres renseignements

Les projets de recherche peuvent utiliser des renseignements désignés et d'autres types de renseignements comme des données d'enquêtes disponibles à l'Institut, des données collectées par des chercheurs (par exemple auprès de participants recrutés par des chercheurs), des renseignements dont l'accès est autorisé par le directeur des services professionnels d'un établissement de santé en vertu de l'article 19.2 de la *Loi sur les services de santé et les services sociaux* (LSSSS) ou encore des renseignements d'organismes publics qui n'ont pas fait l'objet d'une désignation par le gouvernement. Ces données peuvent être appariées avec des renseignements désignés pour la réalisation d'un projet de recherche une fois les autorisations des détenteurs obtenues.

Si un chercheur désire inclure au fichier de recherche des données qui ne sont pas disponibles à l'Institut, il est de sa responsabilité de prendre contact avec le détenteur de ces données afin de s'assurer de leur disponibilité et d'entreprendre les démarches nécessaires pour obtenir les autorisations requises pour y accéder[9].

Les données ajoutées ne pourront en aucun cas contenir des renseignements permettant d'identifier directement une personne. Une attention particulière est accordée à cet élément afin de respecter les obligations de l'Institut en matière de protection des renseignements personnels. Le cas échéant, certains fichiers de données pourraient être refusés s'ils ne permettent pas à l'Institut de respecter ses obligations.

9. Le chercheur doit présenter une demande au gestionnaire des autorisations d'accès aux renseignements de l'organisme concerné.

7 Cycle de vie des renseignements

Les sections qui suivent décrivent les principales étapes liées aux renseignements désignés par le gouvernement, à savoir leur acquisition, leur utilisation, leur conservation et leur destruction.

7.1 Acquisition

En vertu de l'article 13.2 de la LISQ, « *Un organisme public doit, sur demande de l'Institut, lui communiquer les renseignements désignés qu'il détient…* ». Cet article de loi permet à l'Institut de remplir sa mission consistant à assurer la communication, à des fins de recherche, de renseignements détenus par des organismes publics aux chercheurs liés à un organisme public.

L'acquisition par l'Institut des renseignements désignés se fait généralement en établissant une connexion directe avec l'environnement technologique de l'organisme public détenteur des renseignements. Lorsqu'un tel accès n'est pas en place, l'Institut privilégie l'utilisation de sa plateforme Web d'échange d'information sécurisée pour recevoir les données externes nécessaires à la production d'un fichier de recherche. La Procédure pour la transmission électronique des données à l'ISQ établit les règles et les pratiques adéquates pour l'échange de données de façon électronique (site d'échange sécurisé). Cette procédure est appelée à être mise à jour prochainement.

Advenant l'impossibilité d'employer cette plateforme pour le transfert de renseignements, l'Institut peut convenir avec le détenteur des données d'une autre modalité, tant que celle-ci assure une protection des renseignements personnels proportionnelle à leur degré de sensibilité et qui est jugée satisfaisante par l'Institut.

Évaluation des facteurs relatifs à la vie privée

Il est important de souligner que les exigences des articles 13.7 à 13.11 de la LISQ sont équivalentes à celles des articles 67.2.1 à 67.2.3 de la *Loi sur l'accès*. Par conséquent, on peut conclure que l'Institut exige que soient démontrées par le chercheur, et donc évaluées par l'Institut, les conditions que l'on retrouve dans une évaluation des facteurs relatifs à la vie privée (EFVP) pour chacun des projets de recherche qui lui est soumis.

Par ailleurs, une EFVP doit être réalisée pour un projet de recherche lorsque celui-ci requiert la communication d'autres renseignements que ceux désignés par le gouvernement et détenus par un organisme public. Pour être pleinement utile, une EFVP doit être réalisée en amont du projet, et toutes les parties prenantes de l'organisme doivent y participer.

7.2 Utilisation

Cette section couvre les étapes liées à l'utilisation des renseignements désignés à des fins de recherche. Il y est question, entre autres, des obligations de l'Institut pour respecter sa mission de favoriser leur utilisation. Les paragraphes qui suivent aborderont le développement d'outils pour standardiser les demandes d'accès par les chercheurs, de même que la simplification du processus d'approbation faite conformément au nouveau modèle d'accès choisi par le gouvernement.

Demandes d'accès à des renseignements désignés pour la recherche

L'Institut a mis en place un processus simplifié pour aider les chercheurs admissibles qui désirent accéder à des renseignements désignés. Ce processus exige que le chercheur soumette une demande d'accès sur le site Web des services d'accès aux données de recherche de l'Institut. Il doit dans un premier temps s'y ouvrir un compte dans la « Zone recherche », où il sera appelé à s'identifier et à désigner son organisme de rattachement principal. Une fois ce compte créé, il doit ensuite remplir un formulaire de demande d'accès spécifique au projet de recherche concerné[10]. Il doit également joindre à ce formulaire tous les documents nécessaires à l'évaluation de la demande. Ces étapes de même que le cheminement d'une demande d'accès sont représentées dans le schéma de la page suivante.

Afin que l'Institut établisse un contrat d'accès avec un chercheur admissible et son organisme de rattachement, une demande d'accès doit d'abord être examinée par une équipe constituée à cette fin. Cette équipe réalisera une évaluation standardisée pour répondre aux obligations de la LISQ, ce qui lui permettra de recommander la demande au responsable de la protection des renseignements personnels.

Évaluation de la demande

Quatre aspects doivent faire l'objet de cette évaluation :

1. la recevabilité, qui permet de déterminer si le chercheur est admissible à recevoir les services selon les critères définis dans la LISQ. Elle permet également d'établir si la demande respecte les conditions requises ;
2. la faisabilité technique, qui permet d'établir la disponibilité des renseignements demandés pour la période à l'étude. La possibilité de créer un fichier de recherche répondant aux besoins du chercheur tout en respectant les conditions de confidentialité et de protection des renseignements personnels en vigueur à l'Institut est également évaluée ;
3. la faisabilité logistique, qui permet de vérifier la disponibilité des ressources et des moyens techniques (documentation, espaces de travail, logiciels, etc.) et de confirmer la capacité de les mobiliser rapidement afin de répondre aux besoins dans des délais raisonnables ;
4. la vérification de la conformité aux critères entourant la protection des renseignements personnels (PRP), étape qui permet de réduire le risque d'atteinte à la vie privée. Ces critères établissent dans quel cas il est justifié de fournir les renseignements demandés et régissent les différentes conditions encadrant l'accès à ces renseignements, y compris le cadre légal en vigueur. Cette analyse comprend également la vérification de la validité et de l'applicabilité des autorisations fournies par les chercheurs.

Le processus d'évaluation peut comprendre une demande d'avis au Comité d'examen Confidentialité (CEC) de l'Institut ou l'obtention d'une autorisation d'un détenteur externe, lors d'une demande où des renseignements non désignés par le gouvernement sont en cause.

Les différents éléments évalués sont consignés dans un rapport dont la conclusion prend la forme d'une recommandation adressée à la responsable de la protection des renseignements personnels de l'Institut.

10. Le gabarit du formulaire de demande est présenté en annexe 8.

Processus d'accès aux données de recherche – Évolution d'une demande d'accès

	Soumission d'une demande d'accès	Évaluation de la demande	Engagements contractuel et administratif	Préparation du fichier de recherche	Accès au fichier de recherche, exploitation des données et diffusion de résultats	Suivi du projet	Fermeture du projet
Équipe de recherche	▸ Explorer les banques de données ainsi que les variables disponibles et consulter la trousse de démarrage ▸ Effectuer une simulation de coûts, si souhaité ▸ Préparer la demande (formulaire, pièces justificatives et liste de vérification des documents) ▸ S'assurer que tous les documents soumis sont présents et à jour ▸ Soumettre la demande dans la Zone recherche	▸ Fournir les documents et les informations demandés par l'ISQ aux fins de l'évaluation de la demande ▸ Le cas échéant, obtenir les autorisations nécessaires à l'ajout, au fichier de recherche, de données externes	▸ Prendre connaissance des règles de sécurité et de protection des renseignements personnels contenues dans le contrat ▸ Signer le contrat et l'engagement à la confidentialité (équipe de recherche et organisme de rattachement)		▸ Participer à la séance d'orientation tenue par l'ISQ (équipe de recherche) ▸ Se prêter à l'assermentation ▸ Consulter le fichier de recherche dans un environnement sécurisé (dans un CADRISQ ou à distance) ▸ Exploiter les données ▸ Diffuser uniquement des résultats statistiques respectant les règles de confidentialité de l'ISQ	▸ S'assurer que le renouvellement de l'approbation éthique du projet est fourni tout au long de la période d'accès autorisée ▸ À la fin de la période d'accès autorisée, demander une prolongation si la recherche n'est pas terminée ▸ Informer l'ISQ des productions scientifiques découlant de l'exploitation du fichier de recherche	▸ Informer l'ISQ de la fin du projet de recherche nécessitant l'exploitation du fichier de recherche et l'autoriser à entamer la fermeture du projet ▸ Remettre à l'ISQ l'ensemble des éléments d'authentification fournis aux personnes autorisées
Institut de la statistique du Québec (ISQ)	▸ Accompagner le chercheur dans la définition de ses besoins	▸ Évaluer la faisabilité technique de la demande et la disponibilité des données ▸ Estimer, si nécessaire, la taille de la cohorte ▸ Fournir une évaluation sommaire des coûts au chercheur ▸ Évaluer la protection des renseignements personnels ▸ Informer le chercheur des modalités d'accès aux données	▸ Préparer et transmettre le contrat et l'engagement à la confidentialité ▸ Signer le contrat	▸ Procéder à la sélection des individus visés pour la recherche parmi les banques de données sous sa responsabilité ▸ Procéder à l'appariement des banques de données, si nécessaire (méthode probabiliste) ▸ Sélectionner et extraire les variables autorisées ▸ Créer le fichier de recherche pour le projet	▸ Tenir une séance d'orientation obligatoire destinée à l'équipe de recherche (sécurité, protection des renseignements personnels et règles de contrôle du risque de divulgation) ▸ Assermentation de l'équipe de recherche ▸ Fournir aux chercheurs un environnement sécurisé pour accéder aux données, dans lequel des logiciels statistiques sont mis à leur disposition (ex. : STATA, R, SAS, SPSS) ▸ Rendre accessibles le fichier de recherche et les résultats statistiques des travaux du chercheur, selon les modalités convenues ▸ Vérifier les résultats statistiques avant leur diffusion pour s'assurer qu'ils respectent les règles de confidentialité de l'ISQ	▸ Inscrire au dossier du projet les renouvellements d'approbation éthique obtenus par le chercheur ▸ Publier les références des productions scientifiques découlant de l'exploitation des données sur le site Web des services d'accès aux données	▸ Désactiver les accès du chercheur et de son équipe ▸ Détruire les données selon les modalités convenues ▸ Conserver les programmes et la documentation propres au projet à la demande du chercheur

Modalités d'accès aux renseignements désignés par le chercheur

Les services d'accès aux données de recherche de l'Institut offrent différentes options adaptées pour l'utilisation des données de recherche aux chercheurs dont le projet a été approuvé par l'Institut. Les mesures de sécurité mises en place pour l'hébergement, le transfert et l'analyse des données, de même que pour la diffusion des résultats d'analyse, sont proportionnelles au risque de réidentification associé au fichier de recherche.

L'Institut, qui dispose d'une expertise en matière d'accès aux données et de respect des mesures de protection des renseignements personnels, s'assure que les renseignements mis à la disposition des chercheurs sont toujours dépersonnalisés et respectent le niveau de risque de divulgation autorisé.

Accès dans les centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ)

À l'Institut, les chercheurs peuvent accéder aux renseignements désignés autorisés pour leur projet de recherche via un réseau de Centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ), implantés dans certaines universités et institutions publiques. La liste des points d'accès est accessible sur le site Web des services d'accès aux données de recherche au statistique.quebec.ca/recherche/#/nous-joindre.

Ces points d'accès leur permettent de consulter les fichiers de recherche de leur projet à partir de postes informatiques dotés de logiciels statistiques dans un environnement sécurisé par l'Institut. De plus, un analyste-conseil est présent pour s'assurer du respect des consignes et pour répondre à certains besoins des chercheurs.

Accès à distance

L'Institut offre également un accès à distance aux utilisateurs de ses services d'accès aux données à des fins de recherche. Cet accès à distance est régi par des mesures légales et informatiques semblables à celles en place dans un CADRISQ[11].

S'ils sont assortis de mesures de sécurité physique plus souples, les fichiers de microdonnées accessibles à distance (FMAD) peuvent toutefois contenir certains renseignements qui ont été modifiés en vue d'assurer la protection des renseignements personnels. Ce contrôle vise à ce que le risque qu'un utilisateur puisse reconnaître involontairement un ou des individus ne soit pas trop élevé. D'autres organismes de statistique appliquent également un traitement similaire ou des mesures additionnelles à tous les fichiers de microdonnées accessibles à l'extérieur de leurs locaux. Le traitement appliqué au fichier est propre à chaque projet de recherche et tient compte des besoins du chercheur.

Accès dans les locaux de l'organisme de rattachement du chercheur

Pour la grande majorité des projets de recherche, l'accès aux renseignements est autorisé sans le consentement des personnes sur lesquelles portent ces données. Toutefois, pour certains projets, la recherche nécessite un contact avec les personnes visées. Dans ce cas, un consentement à la collecte d'information, à l'utilisation, au jumelage et au partage des renseignements, ou à la conservation des données dans un environnement sécurisé spécifique peut être obtenu.

À titre d'organisme statistique, l'Institut doit respecter le consentement donné par les personnes visées par les projets de recherche. Par conséquent, lorsque le chercheur soumet un projet de recherche pour lequel le consentement requis est réputé être valide et le lieu de conservation des données est explicitement spécifié, l'Institut peut communiquer les renseignements désignés autorisés pour la recherche directement dans l'environnement sécurisé de l'organisme de rattachement du chercheur si celui-ci est reconnu comme étant sécuritaire selon les standards en vigueur à l'Institut.

Malgré tout, l'Institut souhaite inciter les chercheurs qui auront obtenu un tel consentement à utiliser l'environnement sécurisé d'accès à distance de l'Institut pour bénéficier d'un accès à un fichier maître plutôt que d'un accès à un FMAD.

11. Les obligations légales interdisent entre autres aux utilisateurs toute tentative d'identification dite volontaire.

La prochaine section présente les différentes mesures de sécurité que doivent respecter les chercheurs lors de l'utilisation des fichiers de recherche créés à partir des renseignements désignés.

Mesures de sécurité

L'environnement sécurisé a été conçu de façon à répondre à des normes de sécurité élevées, mais aussi de manière à maintenir un équilibre entre la quantité de renseignements disponibles et les obligations à l'égard de la confidentialité des données et de la protection des renseignements personnels. De ce fait, les mesures de sécurité de cet environnement, qui sont à la fois physiques et informatiques, varient selon la modalité d'accès retenue (proportionnalité).

Sécurité physique

L'Institut dispose d'une Politique de sécurisation des locaux, et les CADRISQ sont conçus de façon à respecter les exigences de celle-ci. Parmi les dispositions de la politique, on compte différentes mesures qui visent à réduire l'accès aux personnes non autorisées, et qui portent sur des points comme l'aménagement des postes de travail et l'accès aux locaux restreint aux personnes détentrices d'une carte d'accès et dûment identifiées. D'ailleurs, la fréquentation des locaux est consignée dans des registres automatisés.

Afin de protéger la confidentialité des données rendues accessibles par l'Institut, les appareils électroniques personnels tels que les ordinateurs portables, les tablettes, les téléphones ou tout autre appareil permettant de prendre des photos ou de transmettre des informations par Internet ne sont pas autorisés dans les zones d'accès aux données du CADRISQ.

Sécurité informatique

Les renseignements accessibles pour la recherche sont traités et stockés sur un réseau interne à accès très restreint, uniquement accessible au personnel participant à la production des fichiers de recherche. Tous les documents sensibles liés à ces travaux de production sont sécurisés dans un environnement interne prévu à cette fin.

La plateforme informatique d'accès aux fichiers de recherche est basée sur une infrastructure de bureau virtuel (VDI) de façon à ce qu'il n'y ait aucune donnée stockée sur les postes servant à la consultation des renseignements. Ainsi, le fichier de recherche et la documentation sont conservés uniquement dans l'environnement d'accès sécurisé de l'Institut. Les données sont cloisonnées par projet et ne sont accessibles qu'aux personnes autorisées pour le projet concerné. Ainsi, un chercheur qui a plus d'un projet de recherche possède des comptes distincts qui ne peuvent être accessibles simultanément.

Les comptes utilisateurs sont créés uniquement lorsqu'un contrat est signé. L'accès à l'environnement sécurisé est protégé par une double authentification, et est désactivé à la date d'expiration du contrat. La configuration des mots de passe doit être conforme aux normes établies par l'Institut. Les accès aux environnements sécurisés de l'Institut sont journalisés et un enregistrement visuel des sessions est effectué.

De plus, une liste de contrôle des accès limite les privilèges d'accès nécessaires pour un utilisateur, et des dispositifs technologiques sont en place pour protéger les données de toute intrusion ou action non autorisée.

Contrats avec le chercheur et avec son organisme de rattachement

Le chercheur qui accède à des renseignements désignés et les utilise doit le faire conformément aux conditions et aux modalités prévues au contrat d'accès. Lorsque le projet nécessite des travaux propres à la création du fichier de recherche, ce qui est toujours le cas lorsque des renseignements désignés sont demandés, un second contrat (dit *contrat de service*) doit aussi être signé.

Contrat d'accès

Le contrat d'accès a pour objet d'établir les droits et obligations des parties signataires ainsi que les modalités d'accès au fichier de recherche produit par l'Institut. Il précise entre autres :

- les obligations de l'Institut et celles du chercheur et de son organisme de rattachement ;
- les modalités pour l'accès au fichier de recherche et son utilisation ;

- les renseignements inclus dans le fichier de recherche pour lesquels la nécessité a été justifiée et qui sont autorisés dans le cadre du projet, ainsi que la propriété matérielle et intellectuelle du fichier de recherche et de tous les produits (résultats, tableaux, etc.) dérivés de ce fichier ;
- la durée de l'accès et des obligations du chercheur et de son organisme de rattachement pendant et après la période d'accès ;
- le fait que le chercheur et les personnes de son équipe susceptibles d'exploiter le contenu du fichier de recherche et, par conséquent, de diffuser des résultats, doivent tous signer un formulaire d'engagement à la confidentialité afin d'être autorisés à accéder au fichier de recherche ;
- la nature de l'engagement à la confidentialité du chercheur et des personnes autorisées à accéder au fichier de recherche.

Le chercheur principal et les personnes autorisées doivent prêter serment en vertu de la LISQ. Cet engagement confirme la volonté des chercheurs à respecter les règles de confidentialité et de sécurité des renseignements et de se soumettre aux sanctions prévues à la LISQ en cas de manquement.

Le contrat d'accès doit être signé par le chercheur responsable du projet de recherche ainsi que par son organisme de rattachement, qui doit être un organisme public reconnu par la *Loi sur l'accès*. Par la signature du contrat d'accès, le chercheur responsable du projet et son organisme de rattachement s'engagent à respecter et à faire respecter les règles d'utilisation du fichier de recherche prévues au contrat.

Le chercheur, l'organisme de rattachement ou la personne autorisée à accéder au fichier de recherche qui contrevient aux obligations prévues au contrat s'expose aux sanctions suivantes :

- le retrait de l'accès à l'environnement sécurisé de l'Institut, y compris au fichier de recherche ;
- le refus par l'Institut de conclure tout autre contrat de même nature avec le chercheur ;
- la poursuite du chercheur ou de son organisme de rattachement en vertu des dispositions pénales prévues aux articles 41, 42 et 42.1 de la LISQ ou des dispositions similaires de la *Loi sur l'accès*.

Contrat de service

Le contrat de service est une convention signée entre l'Institut, le chercheur et son organisme de rattachement pour la réalisation de services professionnels, au sens de la *Loi sur les contrats des organismes publics*[12]. Il fournit de l'information au chercheur sur la nature des travaux effectués par l'Institut pour la conception du fichier de recherche autorisé, les coûts associés à ces travaux ainsi que l'échéancier des livrables. Il établit les droits et les responsabilités des parties et précise que l'Institut effectue les travaux conformément aux conditions énoncées dans le contrat d'accès.

Formation et diffusion des résultats

Toute personne autorisée qui veut accéder au fichier de recherche doit suivre une formation obligatoire sur les règles de contrôle du risque de divulgation de renseignements. Un guide d'orientation portant sur ces règles est fourni lors de cette séance.

Cette formation porte notamment sur l'analyse du risque de divulgation que présentent les tableaux et des figures destinés à être diffusés[13]. Des règles spécifiques aux données administratives et aux données d'enquêtes sont aussi précisées[14]. Ces règles sont établies dans la Politique relative à la confidentialité des tableaux de résultats pour diffusion de l'Institut[15].

En prêtant serment, le chercheur s'engage à respecter les exigences en matière de confidentialité de la LISQ. Ce serment est à durée illimitée. Après la fermeture du projet de recherche, le chercheur doit honorer son serment et protéger la confidentialité de tout renseignement auquel il a eu accès dans le cadre de son projet de recherche, même s'il n'occupe plus les mêmes fonctions au sein de son organisme de rattachement.

12. RLRQ, chapitre C-65.1.
13. On considère qu'un résultat est diffusé lorsqu'il sort de l'environnement sécurisé de l'Institut.
14. Au besoin, voir le *Guide à l'intention des chercheurs ; Accès CADRISQ et accès à distance*, p. 21-29.
15. Voir également p. 6 du présent document (section *Politiques et procédures*).

7.3 Conservation et destruction

Dans les pages précédentes, nous avons décrit comment l'Institut acquiert, utilise et protège les renseignements désignés obtenus à des fins de recherche. La dernière section de ce document vient encadrer la façon dont l'Institut conserve et détruit les fichiers de microdonnées et les autres produits qui ont été utilisés et, le cas échéant, communiqués aux chercheurs autorisés. La décision de conserver ou de détruire ces renseignements dépend de la nature des données contenues dans les fichiers et de leur utilité pour assurer la reproductibilité de la recherche ou son utilisation secondaire à moindre coût au bénéfice d'autres chercheurs. Les paragraphes qui suivent couvrent ces différentes situations en fonction des obligations légales en vigueur.

Obligations légales

Conformément aux articles 7 et 8 de la *Loi sur les archives* du Québec, l'Institut a établi et tient à jour un calendrier de conservation soumis et approuvé par Bibliothèque et Archives nationales du Québec (BAnQ) qui détermine les périodes d'utilisation et les supports de conservation de ses documents actifs et semi-actifs, et qui indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés. La version actuelle de ce calendrier de conservation a été approuvée par BAnQ le 16 octobre 2015, avant la création du guichet d'accès aux données de recherche, si bien que la production documentaire unique à ce mandat de l'Institut n'y est pas prise en compte. L'Institut entreprend actuellement la mise à jour de son calendrier de conservation, qui tiendra compte de la production documentaire de ses services d'accès aux données de recherche.

L'utilisation et la destruction des renseignements désignés par le gouvernement sont soumises à la *Loi sur l'accès*. Or, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, dont l'ajout à l'article 73 entrera en vigueur le 22 septembre 2023, précise ceci : « Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire, ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la *Loi sur les archives* (chapitre A-21.1) ou du *Code des professions* (chapitre C-26). Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement ». Ainsi, l'Institut aura le choix entre détruire ou anonymiser les fichiers contenant des renseignements désignés pour répondre aux obligations de la *Loi sur l'accès*.

Toutefois, la LISQ, par son article 30.2, vient également encadrer la destruction des renseignements désignés. Cet article prévoit que « l'Institut doit détruire les renseignements personnels qui lui sont communiqués conformément aux articles 8.1 et 13.2 dès qu'ils ne sont plus nécessaires aux fins de l'entente ou du mandat pour lequel ils ont été demandés ». L'article 30.3 de cette loi précise de plus que l'Institut doit établir des règles encadrant sa gouvernance à l'égard des renseignements personnels désignés et que ces règles doivent notamment encadrer la destruction de ces renseignements.

Par ailleurs, l'utilisation et la destruction des données cliniques par l'Institut sont spécifiquement encadrées par l'article 19.3 de la *Loi sur les services de santé et les services sociaux* (LSSSS), laquelle prévoit que « les renseignements ainsi communiqués à l'Institut ne peuvent être utilisés qu'aux fins de cette recherche et doivent être détruits au terme de celle-ci ».

Quant à lui, l'Institut se conforme aussi à la *Loi sur les archives*[16] qui précise, à l'article 7, que « tout organisme public doit établir et tenir à jour un calendrier de conservation qui détermine les périodes d'utilisation et les supports de conservation de ses documents actifs et semi-actifs et qui indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés ».

Les sections qui suivent viennent encadrer ces obligations.

16. RLRQ, chapitre A-21.1.

Application selon le type de document

L'Institut a pour mission d'assurer la protection des renseignements détenus par les organismes publics et désignés par le gouvernement. Il mise sur les compétences de ses employés, sur des processus éprouvés et sur une infrastructure particulière pour sécuriser la conservation des données de recherche.

À ce titre, l'Institut crée des répertoires spécifiques pour les fichiers de renseignements identificatoires pour que seules les personnes concernées y aient accès aux fins de leurs travaux, conformément à la Procédure de gestion des fichiers de renseignements personnels ou d'identification sur support électronique.

La pratique en vigueur à l'Institut consiste à séparer les renseignements identificatoires des autres renseignements désignés nécessaires à la réalisation d'un projet de recherche, puis à les supprimer dès qu'ils ne sont plus nécessaires à la réalisation du projet. Dans certains cas, si l'on désire conserver les renseignements identificatoires pour une utilisation future, par exemple l'appariement avec une autre source de données, il faut les conserver dans un fichier distinct et dans un endroit sécurisé et uniquement accessible aux personnes dont les fonctions le justifient.

Cette section vient établir quels sont les documents, créés ou utilisés lors de la réalisation d'un projet de recherche, qui peuvent être conservés afin de servir à la réalisation d'autres projets de recherche et lesquels doivent être détruits pour respecter nos obligations.

Clés d'appariement

L'une des étapes de la création d'un fichier de recherche concerne l'appariement de fichiers de différentes sources, par exemple la combinaison de données de santé avec des données de l'éducation. Or, pour chaque appariement réalisé entre deux fichiers de données, l'Institut crée un fichier de clés d'appariement, qui contient uniquement les variables de chacune des sources qui permettent d'identifier de façon unique un individu. Chacune de ces variables correspond à un code non significatif et ne constitue pas un renseignement personnel. Soulignons également que l'Institut s'engage à garder confidentiel le numéro unique de l'organisme détenteur et que seuls quelques employés de l'Institut ayant pour fonction la création ou la gestion des clés d'appariement ont accès à celles-ci.

Cette conservation des clés d'appariement permet à l'Institut de constituer des Registres de clés d'appariement[17] en vue d'améliorer la qualité et l'efficacité des appariements et d'offrir la création de fichiers de recherche à moindre coût, et ce, en réduisant la communication de renseignements personnels, voire en l'éliminant, puisqu'elle ne s'avère plus nécessaire une fois les fichiers déjà appariés.

Programmes

Les programmes informatiques créés par l'Institut pour la sélection des cohortes de recherche et ceux qu'il crée pour l'extraction des renseignements désignés en vue de la création de fichiers de recherche doivent être conservés pour une période de 10 ans, soit suffisamment longtemps pour permettre leur réutilisation pour d'autres projets de recherche. Ces programmes informatiques peuvent être conservés sur un réseau actif ou être archivés. Après cette période, ils peuvent être détruits.

Étant donné que les renseignements désignés sont rendus accessibles aux chercheurs dans l'environnement sécurisé de l'Institut, il existe également plusieurs programmes créés par les chercheurs eux-mêmes. Ces programmes peuvent également être conservés à la demande des chercheurs pour une période d'un maximum de 10 ans non renouvelables. Le chercheur peut toutefois demander que ses programmes soient sortis de l'environnement sécurisé de l'Institut, après qu'un employé ait vérifié qu'ils respectent les règles de confidentialité de l'Institut et les exigences légales auxquelles le chercheur a consenti.

Résultats non diffusés

Les résultats produits par le chercheur lors de ses analyses, mais qui n'ont pas été diffusés, c'est-à-dire qui n'ont pas été sortis de l'environnement sécurisé de l'Institut pendant la période d'accès au fichier de recherche accordée au chercheur, peuvent être conservés à la demande de ce dernier pour une période maximale de

17. Il existe un registre des clés d'appariement entre le FIPA et le RED-décès, un registre des clés d'appariement entre le MEQ et le FIPA, un registre des clés d'appariement entre le FIPA et le RED-naissances vivantes, etc.

trois ans. Après ce délai, les résultats seront détruits. En tout temps, avant cette destruction, le chercheur peut demander qu'un résultat soit sorti de l'environnement sécurisé (c'est-à-dire diffusé). Le cas échéant, un employé de l'Institut devra s'assurer que la demande respecte les règles de confidentialité de l'Institut au moment de la demande de diffusion.

Fichiers des renseignements désignés de l'organisme détenteur

Les fichiers des renseignements désignés de l'organisme détenteur sont généralement accessibles directement via l'environnement sécurisé de l'organisme détenteur. Malgré cela, certains fichiers sont directement transmis à l'Institut de façon ponctuelle. Ceux-ci sont enregistrés dans des répertoires spécifiques qui ne sont pas associés à un projet de recherche en particulier, car ils peuvent être utilisés dans plusieurs projets. L'accès à ces répertoires est restreint aux employés de l'Institut qui collaborent à la gestion et au traitement de ces fichiers.

Lorsqu'une mise à jour d'un fichier déjà transmis est envoyée à l'Institut, une copie du fichier avant la mise à jour est conservée pour une période de 3 mois après la réception d'une nouvelle version. Une fois la conformité de ce nouveau fichier vérifiée, la copie est détruite conformément à la Procédure de gestion des fichiers de renseignements personnels ou d'identification sur support électronique de l'Institut.

Fichiers de sources externes (données cliniques, renseignements non désignés d'un organisme public, données provenant de cohortes formées par des chercheurs)

Les fichiers de sources externes, comme les données cliniques, les renseignements non désignés d'un organisme public ou les données provenant de cohortes formées par des chercheurs, sont d'abord enregistrés dans des répertoires distincts propres à leur projet de recherche et dont l'accès est restreint aux employés de l'Institut participant à la réalisation du projet. Ils sont conservés pour toute la durée du projet pour lequel ils sont nécessaires, et ce, jusqu'à cinq (5) ans après la fin de celui-ci, afin de respecter le principe de reproductibilité de la recherche.

Ces fichiers ne peuvent servir à la réalisation d'autres projets sans qu'une nouvelle demande spécifique soit soumise aux services d'accès aux données de recherche de l'Institut et jugée conforme. Une fois que la période d'accès consentie à un chercheur est expirée, l'Institut lui retire l'accès à toutes les données présentes au fichier de recherche et les conserve, puis les détruit selon les modalités et les délais décrits précédemment. Soulignons qu'entre l'échéance de la période d'accès accordée au chercheur et la destruction du fichier de recherche, ce dernier ne sera plus accessible à quiconque sans un nouveau contrat d'accès.

Si le chercheur fait une demande de prolongation pour l'accès aux données de son projet, la durée de conservation sera prolongée pour tenir compte de cette nouvelle échéance. Les données seront ensuite détruites conformément aux obligations légales de l'Institut et à la Procédure de gestion des fichiers de renseignements personnels ou d'identification sur support électronique de l'Institut.

Fichiers des renseignements identificatoires

Les fichiers de renseignements identificatoires sont conservés tant que les exigences opérationnelles le nécessitent. Des procédures de sécurité très particulières s'appliquent pour l'utilisation de ces renseignements. Ces fichiers sont conservés dans des répertoires spécifiques et seulement sur les serveurs de l'Institut. L'accès à ces fichiers est réservé à un nombre limité d'employés dans le cadre de leurs fonctions.

Lorsque des fichiers de données doivent être combinés, il est parfois nécessaire d'utiliser les renseignements identificatoires. Une fois l'appariement réalisé, un numéro unique non significatif est attribué et remplace les renseignements identificatoires. Ces derniers sont ensuite détruits lorsque toutes les validations de la qualité des traitements sont terminées.

Fichiers intermédiaires / de validation

Les fichiers intermédiaires[18] et les fichiers de validation nécessaires à la création du fichier de recherche sont enregistrés dans des répertoires distincts spécifiques au projet de recherche concerné, et l'accès est restreint au

18. On entend par « fichier intermédiaire » un fichier créé lors d'une des étapes de réalisation des travaux menant à la création du fichier de recherche. Ce type de fichier sert généralement à la validation des étapes de réalisation.

personnel autorisé de l'Institut. Ils sont conservés jusqu'à la date d'échéance du contrat d'accès. Ils sont ensuite détruits, contrairement au fichier de recherche qui est conservé pour une période donnée, mais peuvent être recréés au besoin à faible coût.

Fichiers de recherche

Les fichiers de recherche sont enregistrés dans des répertoires distincts spécifiques au projet de recherche concerné, et l'accès est restreint aux personnes de l'équipe de recherche autorisées et au personnel de l'Institut qui doit fournir du soutien relativement à ces fichiers. Ils sont accessibles à ces personnes dans l'environnement sécurisé des CADRISQ pour toute la durée du projet. Tout comme pour les fichiers de source externe, une fois le contrat d'accès expiré, l'Institut retire au chercheur l'accès au fichier de recherche et conserve ce dernier pour une période allant jusqu'à sept (7) ans afin de respecter le principe de reproductibilité de la recherche, puis le fichier est détruit conformément à la Procédure de gestion des fichiers de renseignements personnels ou d'identification sur support électronique de l'Institut. Là encore, entre l'échéance de la période d'accès accordée au chercheur et la destruction du fichier de recherche, ce dernier ne sera plus accessible à quiconque sans un nouveau contrat d'accès approprié.

Copies de sauvegarde

La Procédure pour l'entreposage des données des serveurs de l'Institut[19] définit l'endroit où doivent être entreposées les données des réseaux et regroupe les règles d'entreposage des copies de sécurité et les règles de destruction de celles-ci.

La destruction d'un renseignement désigné entraîne celle de toutes ses copies, quel que soit le support, et ce, de manière irréversible. L'Institut attribue une balise de sauvegarde à tous les répertoires contenant des renseignements désignés. Cette balise sert à chiffrer chaque copie de sauvegarde effectuée de ce répertoire. Au moment de la destruction des renseignements désignés contenus dans ce répertoire, la balise de chiffrement ayant servi à sécuriser la copie de sauvegarde est également détruite, ce qui rend impossible la récupération des données sur la copie de sauvegarde. Chaque répertoire principal de chaque projet de l'Institut, dont tout projet de recherche, possède sa propre balise de sauvegarde.

19. Une révision de cette procédure est en cours.

Glossaire des termes

Analyse du risque de divulgation : Vérification visant à évaluer le risque de dévoiler une information confidentielle lors de la diffusion (dans un tableau, un modèle, un graphique, etc.) d'un résultat statistique, ou, autrement dit, lors de la sortie d'un tel résultat hors de l'environnement sécurisé de l'Institut.

Données administratives : Traditionnellement, la définition de données administratives englobait les données recueillies et conservées par des organismes publics (UNECE 2011). Une définition élargie existe toutefois depuis quelques années afin d'inclure tout type de données non collectées initialement à des fins statistiques (Conference of European Statisticians). Les données de sources administratives selon la définition traditionnelle forment ainsi un sous-ensemble de ces données. À l'heure actuelle, l'exploitation de sources provenant des différents ministères et organismes publics québécois est toutefois encore la plus répandue.

Donnée clinique : Renseignement provenant du dossier médical d'un patient d'un établissement de santé régi par la *Loi sur les services de santé et les services sociaux* (RLRQ, chapitre S-4.2) et dont l'accès est autorisé par le directeur des services professionnels pour des fins de recherche en vertu de l'article 19.2.

Évaluation des facteurs relatifs à la vie privée (EFVP) : Processus permettant de déterminer si certains projets impliquant l'utilisation de renseignements personnels présentent des risques en matière de protection de la vie privée. L'EFVP permet de détecter ces risques et de proposer des solutions visant à les éliminer ou à les réduire.

Fichier administratif : Fichier constitué aux fins de l'administration de divers programmes non statistiques. Par exemple, des renseignements de nature administrative sont conservés pour satisfaire aux exigences légales de l'enregistrement de certains événements, comme les naissances et les décès, et pour administrer le système de santé et les avantages sociaux (p. ex. les prestations de retraite).

Fichier dépersonnalisé / dénominalisé : Fichier dans lequel les renseignements nominatifs (p. ex. noms, adresses, numéros d'assurance sociale) permettant d'identifier un individu ou un ménage de manière directe ont été retirés.

Fichier de recherche / fichier maître : Fichier contenant l'ensemble des informations sans identifiant direct pour lesquelles un accès a été accordé au demandeur. Il a uniquement été dépersonnalisé, aucun autre traitement visant à réduire le risque d'identification n'a été appliqué aux données qu'il renferme.

Fichier de microdonnées accessible à distance (FMAD) : Fichier contenant les informations sans identifiant direct pour lesquelles un accès a été accordé au demandeur et qui ont fait l'objet d'un traitement visant à réduire le risque d'identification des individus ou des entreprises présents au fichier.

Gouvernance : Ensemble des règles et des processus collectifs, formalisés ou non, par lequel les acteurs concernés participent aux décisions et à la mise en œuvre des actions publiques. Ces règles et ces processus, comme les décisions qui en découlent, sont le résultat d'une négociation constante entre les multiples acteurs impliqués[1].

Identifiant indirect : Information pouvant potentiellement permettre d'identifier une personne, notamment lorsqu'elle est combinée avec d'autres informations de même nature (p. ex. le sexe, l'âge, la profession).

Masquage : Traitement visant à modifier, à supprimer ou à cacher une information contenue dans un fichier de microdonnées ou un tableau de résultats afin de rendre très difficile ou impossible l'identification d'individus ou de ménages. Les techniques suivantes peuvent être utilisées pour masquer certaines informations : regroupement de modalités, suppression d'une variable d'un fichier, suppression d'information pour certains individus, regroupement de valeurs extrêmes, arrondissement ou ajout d'un bruit aléatoire pour des variables quantitatives.

Microdonnées : Données portant sur des individus ou des entreprises. Il peut s'agir de données d'enquêtes, de données administratives ou de données provenant de différentes sources combinées.

Renseignement désigné : Renseignement d'un organisme public dont l'utilisation par l'Institut de la statistique du Québec et la communication à des fins de recherche aux chercheurs liés à un organisme public est permise par un décret gouvernemental.

Renseignement anonymisé : Un renseignement est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier, directement ou indirectement, la personne concernée. Un renseignement anonymisé ne serait plus un renseignement personnel et ne serait donc plus visé par les dispositions des lois sur la protection des renseignements personnels.

Renseignement dépersonnalisé : Un renseignement est dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée. Il s'agit d'un renseignement dont les identifiants directs (nom, prénom, adresse, numéro d'assurance sociale, numéro d'assurance maladie) ont été retirés. Ces renseignements demeurent des renseignements personnels et sont soumis aux dispositions des lois sur la protection des renseignements personnels.

Renseignement identificatoire / nominatif / Identifiant direct : Renseignement permettant d'identifier un individu ou une entreprise de manière directe (p. ex. nom, adresse, numéro de téléphone, numéro d'assurance sociale, numéro d'entreprise du Québec).

Renseignement personnel : Renseignement qui porte sur une personne physique et qui permet, seul ou en combinaison avec d'autres renseignements, de l'identifier.

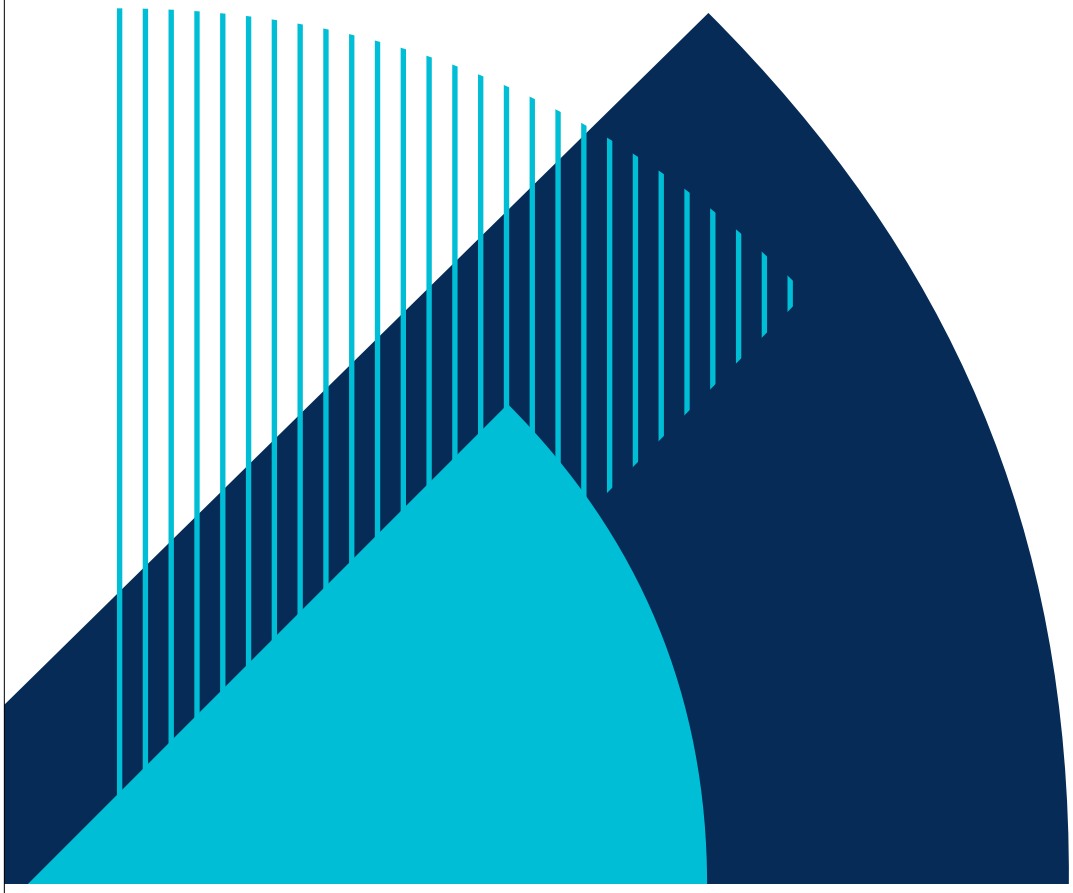
Résultat intermédiaire : Résultat statistique produit lors d'analyses préliminaires qui ne sont pas destinées à la diffusion et qui demeurent dans l'environnement sécurisé de l'Institut.

1. Isabelle LACROIX et Pier-Olivier ST-ARNAUD (2012), « La gouvernance : tenter une définition », *Cahiers de recherche en politique appliquée*, vol. IV, numéro 3, 26.

Annexes

Annexe 1

Politique d'accès aux microdonnées portant sur des individus ou des ménages



INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Note

La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes.

Date d'approbation :	9 avril 2001
Dernière mise à jour :	11 janvier 2021
Unité responsable de la mise à jour :	Direction de la méthodologie

1 Objectif

Soucieux de contribuer au développement des connaissances pour la société québécoise, l'Institut de la statistique du Québec (ISQ) offre un ensemble de services pour faciliter l'accès aux microdonnées à des fins de recherche scientifique. En raison des nouvelles responsabilités qui lui ont été confiées par le gouvernement du Québec à l'égard des données administratives des ministères et organismes, l'ISQ a mis en place un guichet de services constituant la porte d'entrée pour accéder aux microdonnées provenant de ses propres enquêtes et de fichiers administratifs.

La présente politique concerne uniquement l'accès aux microdonnées portant sur des individus ou des ménages. Y sont présentés les différents types de microdonnées produites par l'ISQ ainsi que la procédure à suivre pour y accéder.

2 Types de microdonnées et modes d'accès

Fichier maître

Un chercheur ou un organisme public peut uniquement accéder à un fichier maître (c'est-à-dire contenant des microdonnées détaillées) dans un Centre d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ)[1]. Ce type de fichier comporte un potentiel analytique élevé du fait qu'il soit seulement dénominalisé. En conséquence, des exigences légales et administratives ainsi que des mesures de sécurité physique et informatique sévères sont requises pour encadrer son utilisation et réduire le risque de divulgation d'information confidentielle.

Fichier de microdonnées accessible à distance (FMAD)

Lorsqu'un demandeur le souhaite, il peut accéder à distance à un fichier de microdonnées se trouvant dans un environnement informatique contrôlé et sécuritaire. Des mesures de contrôle statistique de la divulgation sont toutefois appliquées à ces microdonnées en raison du fait que les mesures de sécurité physique visant à les protéger ne sont pas aussi sévères que celles en place dans un CADRISQ[2]. Trois types de FMAD peuvent être produits conformément à la procédure présentée en annexe[3]. L'offre peut ainsi être adaptée aux besoins du demandeur.

Fichier de microdonnées à grande diffusion (FMGD)

Pour des données d'enquêtes de l'ISQ uniquement, un FMGD peut être produit. Pour la création d'un tel fichier, des méthodes de masquage sévères sont utilisées afin de réduire le risque de divulgation à un niveau acceptable. Le fichier est transmis au demandeur, qui peut alors l'exploiter à même ses locaux.

3 Demande d'accès[4]

Toute demande d'accès doit être effectuée par l'entremise du guichet d'accès aux données de recherche à l'adresse suivante :

statistique.quebec.ca/recherche/#/accueil.

Le demandeur doit d'abord créer un compte utilisateur, puis remplir un formulaire en ligne dans la Zone recherche. Ces étapes doivent être suivies tant pour une demande d'accès à des données d'enquêtes que pour une demande d'accès à des données administratives.

1. Si le demandeur est un organisme public, seul le personnel de cet organisme peut avoir accès aux microdonnées. Exceptionnellement, le fichier maître d'une enquête peut être exploité dans les locaux d'un organisme public ou être accessible à distance lorsque le consentement des répondants à l'enquête a été obtenu.
2. Ces mesures de contrôle statistique visent uniquement à réduire le risque d'identification involontaire, puisque le demandeur s'engage légalement à ne pas tenter d'identifier des individus ou des ménages.
3. Le choix des méthodes de contrôle statistique de la divulgation appliquées à un FMAD se fera en fonction des besoins du demandeur, soit un chercheur ou un organisme public, ainsi que de ceux de la direction responsable du programme auquel les données d'enquêtes sont rattachées.
4. L'accès aux microdonnées recueillies est parfois prévu à l'entente liant l'ISQ et ses partenaires dans la réalisation d'une enquête. Le processus de demande et d'approbation n'a pas à être suivi dans cette situation.

4 Approbation d'une demande d'accès

4.1 Fichier maître ou fichier de microdonnées accessible à distance (FMAD)

Pour toute demande d'accès à des données d'enquêtes de l'ISQ, le comité d'examen doit émettre un avis favorable[5]. Ce comité, convoqué bimensuellement, est composé :

a. d'un représentant du Service d'accès aux données à des fins de recherche (SAD) ;

b. du conseiller juridique de l'ISQ ;

c. du responsable de la protection des renseignements personnels (ou de la personne qu'il délègue à ce comité) ;

d. d'un membre du comité d'éthique de l'ISQ ;

e. du directeur de la méthodologie (ou de la personne qu'il délègue à ce comité) ;

f. du directeur ou de la directrice responsable du programme auquel les microdonnées sont rattachées (ou de la personne qu'il ou elle délègue à ce comité).

Si la demande ne concerne que des données administratives, cet avis du comité d'examen est optionnel. Dans ce cas, c'est plutôt une recommandation qui doit être formulée par le responsable de la protection des renseignements personnels (PRP) (ou par la personne à qui il délègue cette tâche).

Pour fournir un avis éclairé, le comité d'examen ou le responsable de la PRP doit évaluer la demande afin de s'assurer de la faisabilité du projet de recherche et de sa conformité avec la présente politique. Le comité d'éthique, le comité d'examen Confidentialité (CEC) et tout autre intervenant peuvent être consultés au cours de ce processus d'évaluation.

Pour toute demande relative à des données administratives, l'ISQ doit soumettre au nom du demandeur une demande d'autorisation à la Commission d'accès à l'information (CAI) et aux détenteurs de données concernés.

Sur la base de la recommandation du comité d'examen ou du responsable de la PRP, et à la suite de l'obtention de l'autorisation de la CAI et des détenteurs de données lorsque nécessaire, le directeur général de l'ISQ approuve la demande et signe un contrat avec le demandeur. De plus, un formulaire d'engagement à la confidentialité doit être signé par le demandeur et par toute autre personne qui aura accès aux microdonnées.

4.2 Fichier de microdonnées à grande diffusion (FMGD)

L'accès à un tel fichier nécessite l'approbation du directeur ou de la directrice responsable du programme auquel les microdonnées sont rattachées. Un contrat est nécessaire, mais le demandeur n'a pas dans ce cas à signer un formulaire d'engagement à la confidentialité. La demande d'accès doit être soumise au conseiller juridique de l'ISQ, lequel la transmettra aux Publications du Québec.

4.3 Registre des contrats et ententes

Un registre des contrats et des ententes (ainsi que des formulaires d'engagement à la confidentialité) est tenu par le Secrétariat et Affaires juridiques (SAJ) en collaboration avec le SAD.

5. Un tel avis est également nécessaire lorsqu'un demandeur souhaite accéder à des données d'enquêtes de Statistique Canada transmises à l'ISQ en vertu du consentement au partage de renseignements obtenu des répondants.

Annexe – Procédure pour la création d'un fichier de microdonnées[6]

Étapes de création	Types de fichier			
		Fichier de microdonnées accessible à distance (FMAD)[1]		
	Fichier de microdonnées à grande diffusion (FMGD)	Fichier masqué contre l'identification involontaire (FMII)	Fichier de recherche masqué accessible à distance (FRMAD)	Fichier de microdonnées fictif (FMF)
0) Approbation de la demande	• Approbation du directeur ou de la directrice responsable du programme auquel les microdonnées sont rattachées ; • Signature d'un contrat entre le demandeur et l'ISQ.	• Approbation du comité d'examen ou du responsable de la protection des renseignements personnels (PRP) ; • Autorisation de la Commission d'accès à l'information (CAI) et des détenteurs de données (si nécessaire) ; • Signature d'un contrat entre le demandeur et l'ISQ ; • Signature d'un formulaire d'engagement à la confidentialité.	• Approbation du comité d'examen ou du responsable de la protection des renseignements personnels (PRP) ; • Autorisation de la Commission d'accès à l'information (CAI) et des détenteurs de données (si nécessaire) ; • Signature d'un contrat entre le demandeur et l'ISQ ; • Signature d'un formulaire d'engagement à la confidentialité.	• Approbation du comité d'examen ou du responsable de la PRP.
1) Choix du type de fichier	• Le FMGD est privilégié lorsque le demandeur souhaite exploiter les données à même ses locaux.	• Le FMII offre un potentiel analytique semblable à celui du FRMAD. Il est privilégié lorsque que le demandeur ne cherche à accéder qu'à peu de renseignements ou qu'à des données d'enquêtes.	• Le FRMAD offre un potentiel analytique semblable à celui du FMII. Il est privilégié, à moins que le demandeur ne cherche à accéder qu'à peu de renseignements ou qu'à des données d'enquêtes. Le demandeur est sollicité lors de la création d'un FRMAD, notamment pour qu'il modifie les variables trop détaillées lorsque nécessaire.	• Le FMF est un fichier entièrement fictif permettant simplement la préparation de programmes informatiques. Aucune mesure de sécurité physique et informatique n'est nécessaire.

Suite à la page 6

6. Avant de procéder à la création d'un FMGD ou d'un FMAD, la Direction de la méthodologie (DM) doit évaluer la faisabilité de la production d'un tel fichier et les coûts associés.

Étapes de création	Types de fichier			
		Fichier de microdonnées accessible à distance (FMAD)[1]		
	Fichier de microdonnées à grande diffusion (FMGD)	Fichier masqué contre l'identification involontaire (FMII)	Fichier de recherche masqué accessible à distance (FRMAD)	Fichier de microdonnées fictif (FMF)
2) Classement des variables du fichier	• Trois catégories : les identifiants directs, les identifiants indirects et les variables non identificatrices.	• Trois catégories : les identifiants directs, les identifiants indirects et les variables non identificatrices.	• Trois catégories : les identifiants directs, les identifiants indirects et les variables non identificatrices.	• Trois catégories : les identifiants directs, les identifiants indirects et les variables non identificatrices.
3) Application du contrôle statistique de la divulgation (CSD)	3.1) Suppression des identifiants directs.	3.1) Suppression des identifiants directs.	3.1) Suppression des identifiants directs.	3.1) Suppression des identifiants directs.
	3.2) Traitement des dates exactes d'événements (naissance, décès, hospitalisation, etc.) : suppression des dates.	3.2) Traitement des dates exactes d'événements (naissance, décès, hospitalisation, etc.) : ajout d'un bruit aléatoire aux dates de sorte que les délais, la chronologie et les durées sont préservés.	3.2) Traitement des dates exactes d'événements (naissance, décès, hospitalisation, etc.) : ajout d'un bruit aléatoire aux dates de sorte que les délais, la chronologie et les durées sont préservés.	3.2) Traitement des dates exactes d'événements (naissance, décès, hospitalisation, etc.) : les dates sont remplacées par des dates fictives.
	3.3) Mesure du risque d'identification **volontaire** basée sur : • Le nombre d'habitants dans la population d'une région distinguable dans le fichier (le seuil minimal étant de 80 000 habitants) ; • Le nombre d'individus dans la population par combinaison de trois identifiants indirects (le seuil minimal étant de 800 personnes)[3].	3.3) Mesure du risque d'identification **involontaire**[2] basée sur : • La probabilité qu'un individu ou un ménage soit identifié involontairement par le biais des identifiants indirects. Lorsque plus de deux ou trois renseignements sont nécessaires pour identifier un individu ou un ménage, si une identification est faite, elle est considérée comme volontaire; • L'unicité des renseignements fournis par les identifiants indirects.	3.3) Mesure du risque d'identification **involontaire**[2] basée sur : • La probabilité qu'un individu ou un ménage soit identifié involontairement par le biais des identifiants indirects. Lorsque plus de deux ou trois renseignements sont nécessaires pour identifier un individu ou un ménage, si une identification est faite, elle est considérée comme volontaire; • L'unicité des renseignements fournis par les identifiants indirects.	3.3) Aucune mesure du risque d'identification n'est nécessaire étant donné le contrôle appliqué à l'étape 3.4.

Suite à la page 7

Étapes de création	Types de fichier			
		Fichier de microdonnées accessible à distance (FMAD)[1]		
	Fichier de microdonnées à grande diffusion (FMGD)	Fichier masqué contre l'identification involontaire (FMII)	Fichier de recherche masqué accessible à distance (FRMAD)	Fichier de microdonnées fictif (FMF)
3) Application du contrôle statistique de la divulgation (CSD)	3.4) Contrôle du risque de divulgation[4] : • Si nécessaire en fonction de la mesure du risque effectuée à l'étape 3.3, les valeurs de certains identifiants indirects sont masquées pour que le risque d'identification **volontaire** soit considéré comme acceptable.	3.4) Contrôle du risque de divulgation[4] : • Si nécessaire en fonction de la mesure du risque effectuée à l'étape 3.3, les valeurs de certains identifiants indirects sont masquées pour que le risque d'identification **involontaire** soit considéré comme acceptable[5]. • Les caractéristiques uniques ou atypiques pour les identifiants indirects sont masquées.	3.4) Contrôle du risque de divulgation[4] : • Si nécessaire en fonction de la mesure du risque effectuée à l'étape 3.3, les valeurs de certains identifiants indirects sont masquées pour que le risque d'identification **involontaire** soit considéré comme acceptable[5]. • Les caractéristiques uniques ou atypiques pour les identifiants indirects sont masquées.	3.4) Contrôle du risque de divulgation[4] : • Les données du fichier sont fictives, de même que les individus ou les ménages s'y retrouvant. • Les valeurs fictives ne reflètent aucunement la population étudiée par le demandeur.
4) Fichier résultant	• Les identifiants directs sont supprimés ; • Les dates exactes sont supprimées ; • Les valeurs de certains identifiants indirects sont masquées si nécessaire pour réduire le risque d'identification **volontaire** ; • Les autres identifiants indirects ainsi que les variables non identificatrices ne sont pas modifiés.	• Les identifiants directs sont supprimés ; • Les dates exactes sont modifiées par l'ajout d'un bruit aléatoire ; • Les valeurs de certains identifiants indirects sont masquées si nécessaire pour réduire le risque d'identification **involontaire** ; • Les autres identifiants indirects ainsi que les variables non identificatrices ne sont pas modifiés.	• Les identifiants directs sont supprimés ; • Les dates exactes sont modifiées par l'ajout d'un bruit aléatoire ; • Les valeurs de certains identifiants indirects sont masquées si nécessaire pour réduire le risque d'identification **involontaire** ; • Les autres identifiants indirects ainsi que les variables non identificatrices ne sont pas modifiés.	• Les identifiants directs sont supprimés ; • Les dates sont fictives ; • Tous les identifiants indirects et les variables non identificatrices contiennent des valeurs fictives.

1. Les résultats obtenus par l'entremise de l'accès à distance devront être reproduits dans un CADRISQ à l'aide de données du fichier maître si seulement ces résultats portent sur des renseignements modifiés, synthétiques ou fictifs et que le demandeur souhaite les divulguer.
2. L'accès à distance permet d'assouplir les mesures de CSD, notamment en raison des exigences légales et des mesures de sécurité (informatique et physique) importantes requises.
3. La région distinguable doit être l'un des identifiants indirects de la combinaison.
4. Un glossaire se trouvant à l'annexe B présente les techniques de masquage pouvant être employées.
5. Le FRMAD offre la possibilité d'employer des données synthétiques ou fictives pour protéger la confidentialité des renseignements ainsi que d'utiliser des techniques de masquage plus traditionnelles. La création d'un tel fichier peut être retenue notamment lorsque la suppression complète des valeurs de certains identifiants indirects est nécessaire pour réduire le risque d'identification involontaire à un niveau acceptable. Il est à noter que la suppression d'information sur une base individuelle proposée pour le FMII et le FMGD ne s'applique pas pour ce type de fichier.

Glossaire

Bruit aléatoire

Valeur choisie au hasard qui est ajoutée à une information pour la brouiller.

Contrôle statistique de la divulgation (CSD)

Méthodes et procédés mis en œuvre afin de minimiser le risque de divulgation de données lors de la diffusion d'informations statistiques.

Données fictives

Valeurs fictives attribuées à une information afin de masquer les valeurs réelles. Ces valeurs sont des valeurs possibles, mais aucun effort visant à conserver leur utilité statistique n'est consacré dont leur relation avec les autres informations contenues dans le fichier. Elles ne servent qu'à l'élaboration de programmes informatiques. Les résultats produits à partir de données fictives ne reflètent aucunement les résultats qui seront produits à partir du fichier maître.

Données synthétiques

Valeurs plausibles attribuées à une information afin de masquer les valeurs réelles. Des efforts visant à conserver leur utilité statistique sont consacrés dont leur relation avec les autres informations contenues dans le fichier. Elles servent à l'exploration des données et à l'élaboration de programmes informatiques. Les résultats produits à partir de données synthétiques devraient généralement bien refléter les résultats qui seront produits à partir du fichier maître.

Fichier administratif

Fichier constitué aux fins de l'administration de divers programmes non statistiques. Par exemple, des renseignements de nature administrative sont conservés pour satisfaire aux exigences légales liées à l'enregistrement de certains événements, comme les naissances et les décès, et pour administrer le système de santé et les avantages sociaux.

Fichier dénominalisé

Fichier dans lequel les renseignements nominatifs (p. ex., le nom, l'adresse, le numéro d'assurance sociale) permettant d'identifier un individu ou un ménage de manière directe ont été retirés.

Fichier maître

Fichier contenant l'ensemble des informations non nominatives dont l'accès par le demandeur a été autorisé. Il a uniquement été dénominalisé. Aucun autre traitement visant à réduire le risque d'identification n'a été appliqué aux données qu'il contient.

Identifiant direct

Information permettant d'identifier de manière directe une personne ou un ménage (p. ex., le nom, l'adresse, le numéro de téléphone).

Identifiant indirect

Information pouvant permettre potentiellement d'identifier une personne ou un ménage, notamment lorsque combinée avec d'autres informations de même nature (p. ex. le sexe, l'âge, la profession).

Identification involontaire

Identification imprévue ou inattendue d'un individu ou d'un ménage par l'utilisateur d'un fichier. Une telle identification peut se produire lorsque l'utilisateur survole les données et observe certaines caractéristiques inhabituelles qui lui rappellent un individu ou un ménage connu. Les chances qu'une identification involontaire se produise sont plus grandes si l'individu ou le ménage possède des caractéristiques rares connues par l'utilisateur.

Identification volontaire

Identification délibérée d'un individu ou d'un ménage par un utilisateur mal intentionné. Une telle identification peut se produire entre autres lorsque l'utilisateur combine les données d'un fichier à d'autres sources de données ou qu'il recherche des individus ou des ménages atypiques.

Masquage

Traitement visant à modifier, supprimer ou cacher une information contenue dans un fichier de microdonnées ou un tableau de résultats afin de rendre très difficile ou impossible l'identification d'individus ou de ménages. Les techniques suivantes peuvent être utilisées pour masquer certaines informations : regroupement de modalités, suppression d'une variable d'un fichier, suppression d'information pour certains individus, regroupement de valeurs extrêmes, arrondissement ou ajout d'un bruit aléatoire pour des variables quantitatives.

Microdonnées

Données portant sur des individus ou des ménages. Il peut s'agir de données d'enquêtes, de données administratives ou de données provenant de différentes sources combinées.

Utilité des données

Capacité des données à fournir l'information et les résultats souhaités par le demandeur.

Variable non identificatrice

Information ne pouvant permettre, même lorsque combinée avec d'autres informations, d'identifier une personne ou un ménage (ex. : le sexe, l'âge, la profession).

Références bibliographiques

BÉLAND, Y. (1999). "Release of Public Use Microdata Files for NPHS? Mission... partially accomplished!", dans *Proceedings of the Survey Research Methods Section,* American Statistical Association, p. 404-409.

CANADIAN INSTITUTE FOR HEALTH INFORMATION (2010). *"Best Practice" Guidelines for Managing the Disclosure of De-Identified Health Information*, Ottawa, 53 p.

EL EMAM, K. (2013). *Guide to the De-Identification of Personal Health Information*, Boca Raton, CRC Press, 414 p.

SCHULTE NORDHOLT, E. (2001). *Statistical Disclosure Control (SDC) in Practice : Some Examples in Official Statistics of Statistics Netherlands*. [Article présenté à la Joint ECE/Eurostat Work Session on Statistical Data Confidentiality à Skopje, capitale de l'ancienne République yougoslave de Macédoine].

STATISTIQUE CANADA (2016). *Compendium de pratiques de gestion pour les organismes statistiques du Programme international en gestion d'organismes statistiques de Statistique Canada*, produit nº 11-634-X au catalogue de Statistique Canada, Ottawa, Statistique Canada, 288 p.

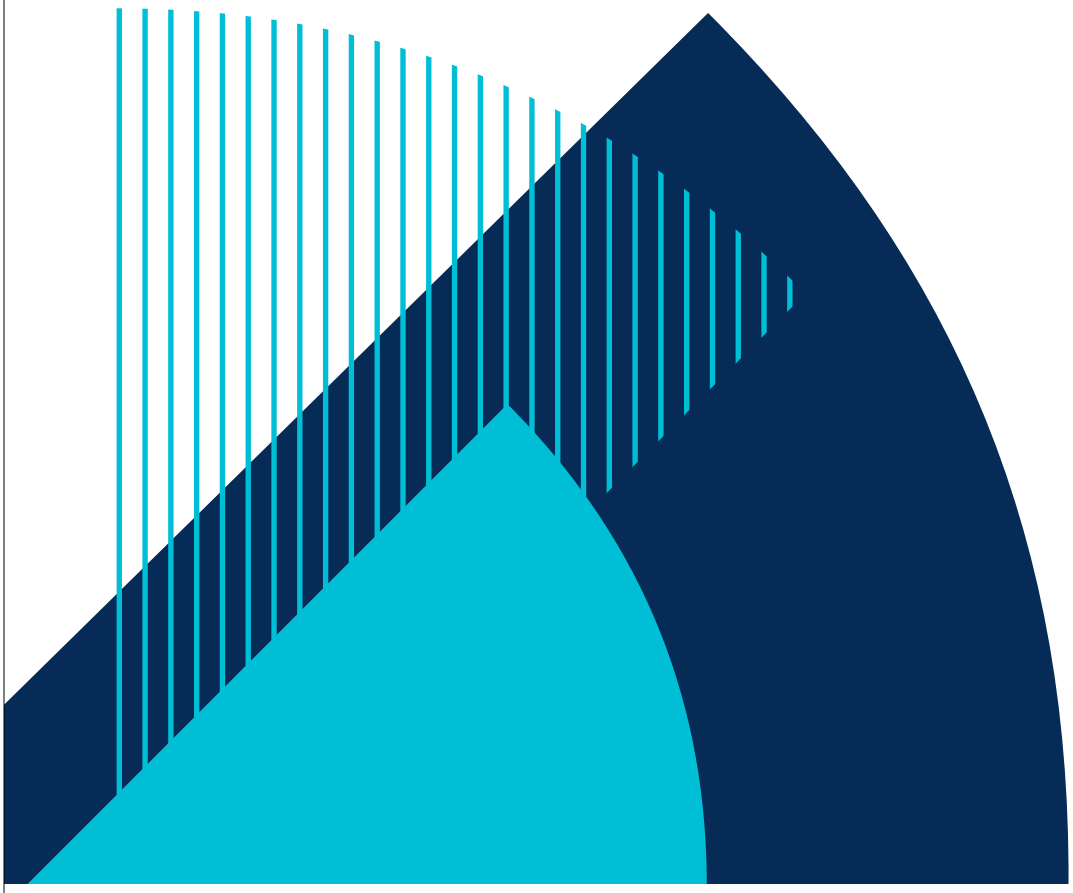
« La statistique au
service de la société :
la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec

Annexe 2

Politique relative à la confidentialité des tableaux de résultats pour diffusion



INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Note

La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes.

Date d'approbation des lignes directrices :	12 octobre 2004
Date de la dernière modification :	Septembre 2021
Unité responsable de la mise à jour :	Direction de la méthodologie

Table des matières

Contexte et objectifs

1. Conformément à sa mission, l'Institut doit exploiter tout le potentiel d'information statistique dont il dispose. Cette information provient des renseignements recueillis dans le cadre des enquêtes qu'il mène auprès des individus, des ménages ou des entreprises, du Registre des événements démographiques et de fichiers administratifs de ministères et d'organismes.

2. L'article 25 de la Loi sur l'Institut de la statistique du Québec (RLRQ, c. I-13.011) prévoit ceci : « Le directeur général, les fonctionnaires et toute autre personne dont les services sont utilisés par le directeur général dans l'exercice de ses fonctions ne peuvent révéler ni faire révéler, par quelque moyen que ce soit, des renseignements obtenus en vertu de [cette] loi si ces révélations permettent de rattacher un renseignement à une personne, à une entreprise, à un organisme ou à une association en particulier. »

3. La présente politique a pour objectif de permettre le contrôle du risque de divulgation de renseignements confidentiels à partir de tableaux de résultats pour diffusion.

Définitions

4. Renseignement confidentiel : Renseignement qui peut être rattaché à une personne, à une entreprise, à un organisme ou à une association en particulier, de façon directe ou indirecte, ce qui entraînerait la divulgation d'une information individuelle.

5. Tableau de résultats : Mode de présentation de données définitives ou préliminaires notamment sous forme de fréquences, de totaux, de moyennes, de ratios, de médianes ou de centiles. Il est à noter qu'un tableau de résultats peut aussi prendre la forme d'un modèle ou d'un graphique.

6. Source des données : Enquête menée auprès des individus, des ménages ou des entreprises, Registre des événements démographiques ou fichier administratif d'un ministère ou organisme.

Orientations générales

7. Le chargé de projet est responsable de l'application de la présente politique lorsque l'Institut diffuse des tableaux de résultats liés à son projet.

8. Certains analystes ou chercheurs externes ont accès aux fichiers de microdonnées de l'Institut en vertu de la Politique d'accès aux microdonnées portant sur des individus ou de ménages de l'Institut. Tous les analystes, chercheurs et assistants susceptibles de diffuser des tableaux de résultats sont considérés comme des personnes « dont les services sont retenus par le directeur général » de l'Institut et sont soumis aux obligations de confidentialité prévues à l'article 25 de la Loi sur l'Institut de la statistique du Québec. Ils sont d'ailleurs tenus de signer un formulaire d'engagement à la confidentialité. Les ententes et les contrats comportent par ailleurs des conditions précises visant à assurer que seuls les analystes ou chercheurs autorisés et leurs assistants ont accès au fichier. En conséquence, ils sont responsables de l'application de la présente politique lorsqu'ils diffusent des tableaux de résultats.

9. Pour contrôler le risque de divulgation de renseignements confidentiels à partir de tableaux de résultats pour diffusion, les diffuseurs potentiels doivent tout d'abord déterminer quels tableaux de résultats comportent des risques de divulgation de renseignements confidentiels, à l'aide des procédures présentées un peu plus loin. Le cas échéant, ils ont deux options :

- ne pas diffuser le tableau ;
- appliquer au tableau une technique adéquate de masquage selon la procédure à suivre.

Un chargé de projet peut choisir d'appliquer des mesures plus sévères que celles détaillées dans la procédure qui le concerne. Au besoin, il peut faire appel aux méthodologistes de la Direction de la méthodologie (DM) pour qu'ils le soutiennent quant à l'application de la procédure à suivre.

Mise à jour

10. La DM est responsable de la mise à jour de la présente politique.

Procédures

11. La source des données, le type de fichier (fichier non masqué ou masqué) et le lieu de conservation du fichier dictent le choix de la procédure à utiliser pour déterminer quels tableaux de résultats comportent des risques de divulgation de renseignements confidentiels. Il en existe huit :

- Procédure pour les tableaux de résultats produits à l'Institut à partir d'un fichier de microdonnées non masquées d'une enquête menée auprès des individus et des ménages : voir l'annexe 1 ;
- Procédure pour les tableaux de résultats produits aux CADRISQ à partir d'un fichier de microdonnées non masquées d'une enquête menée auprès des individus et des ménages : voir l'annexe 2 ;
- Procédure pour les tableaux de résultats produits aux CADRISQ à partir d'un fichier constitué à des fins d'analyse ou de recherche externe (FARE) d'une enquête menée auprès des individus et des ménages : voir l'annexe 3 ;
- Procédure pour les tableaux de résultats produits dans les locaux d'un organisme public à partir d'un fichier FARE d'une enquête menée auprès des individus et des ménages : voir l'annexe 4 ;
- Procédure pour les tableaux de résultats produits dans les locaux d'un organisme public à partir d'un fichier de microdonnées non masquées d'une enquête menée auprès des individus et des ménages (cas particulier après obtention du consentement des répondants pour le partage des données avec un organisme public) : voir l'annexe 5 ;
- Procédure pour les tableaux de résultats produits à l'Institut à partir d'un fichier de microdonnées non masquées d'une enquête menée auprès des entreprises : voir l'annexe 6 ;
- Procédure pour les tableaux de résultats produits à l'Institut à partir du Registre des événements démographiques : voir l'annexe 7 ;
- Procédure pour les tableaux de résultats produits aux CADRISQ ou en accès à distance à partir d'un fichier de données administratives : voir l'annexe 8.

L'information détaillée sur le contrôle du risque de divulgation pour chacune des situations est disponible sur demande.

Annexe 8

Procédure pour les tableaux de résultats produits aux CADRISQ ou en accès à distance à partir d'un fichier de données administratives

Jimmy Baulne, Karine Dion et Éric Gagnon
Direction de la méthodologie
Mai 2021

Conformément à sa mission, l'Institut doit veiller à ce que l'information statistique de ses fichiers de données soit exploitée à son plein potentiel. Les Centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ) jouent un rôle primordial dans l'atteinte de cet objectif. Cependant, en vertu de la Loi sur l'Institut de la statistique du Québec, quiconque dont les services sont retenus par le directeur général ne peut révéler ni faire révéler, par quelque moyen que ce soit, des renseignements recueillis en vertu de cette loi si ces révélations permettent de rattacher un renseignement à une personne, à une entreprise, à un organisme ou à une association en particulier. L'Institut s'est donc doté de règles de confidentialité qui permettent de diminuer le risque de divulgation de renseignements confidentiels lors de la diffusion de résultats.

Résultats produits à partir d'un fichier de données administratives

Le présent document énonce la procédure qu'un utilisateur doit suivre afin de faire approuver, par un responsable de l'Institut, la sortie de ses résultats de recherche produits dans un CADRISQ ou en accès à distance à partir d'un fichier[1] de données administratives.

Lorsque des données administratives sont jumelées avec des données provenant d'une enquête, ce sont les règles de confidentialité qui encadrent l'utilisation des données de l'enquête qui doivent être appliquées.

L'utilisateur pourra constater que les règles à appliquer présentées dans cette procédure peuvent varier en fonction de la banque de données administratives utilisée. En effet, elles dépendent notamment de la provenance des fichiers ainsi que de la nature de l'information qui s'y trouve. Le responsable du CADRISQ veillera dès le début du projet à ce que l'utilisateur ait à sa disposition l'ensemble des règles appropriées pour les banques de données qu'il utilise.

Procédure pour l'analyse du risque

La procédure à suivre pour analyser la confidentialité des résultats de recherche produits se résume comme suit :

1. Sélectionner les résultats à diffuser[2].

2. Vérifier que la taille de la population[3] associée à la zone géographique de diffusion respecte le seuil du critère géographique associé à la banque de données administratives utilisée (voir la section 1 de la présente annexe). Ce critère est établi en fonction de la nature de l'information contenue dans la banque de données.

3. Vérifier le risque de divulgation à l'aide des règles[4] de confidentialité présentées dans la section 2, 3 ou 4 de la présente annexe, lesquelles dépendent de la banque de données administratives utilisée. Le responsable du CADRISQ indiquera à l'utilisateur à quelle section il devra se référer pour son projet.

4. S'il existe un risque de divulgation, appliquer une technique de masquage pour diminuer ce risque. Le regroupement des modalités problématiques est la

1. Ce fichier peut être constitué des données d'une partie seulement ou de l'entièreté de la population visée. Si le fichier de données administratives ne contient qu'un échantillon aléatoire de la population visée, on considère ce fichier comme l'équivalent d'un fichier de données d'une enquête. Dans ce cas, il faut utiliser la procédure relative à la confidentialité des tableaux de résultats produits à partir d'un fichier de microdonnées non masquées d'une enquête menée auprès des individus et des ménages.
2. Notons qu'il est possible d'accéder à certains résultats non masqués en accès à distance pour les opérations de validation, ce qui permet d'éviter de demander la vérification de risque et le masquage de nombreux tableaux. Pour plus d'informations, voir le *Guide à l'intention des chercheurs exploitant des résultats intermédiaires en accès à distance*.
3. La population associée à une zone géographique de diffusion donnée comprend toutes les personnes vivant dans cette zone, et non pas uniquement celles comprises dans le sous-ensemble visé par le projet de recherche. Cette population peut être déterminée à partir des estimations de population basées sur le recensement. Toutefois, si les analyses à effectuer portent sur des travailleurs, la taille de la population doit être établie seulement en fonction des personnes travaillant dans la zone géographique de diffusion. Voir la section 1 à la fin du présent document pour plus d'informations.
4. Les règles relatives à la vérification du risque de divulgation sont présentées sous forme de thèmes, qui sont au nombre de 10.

technique de masquage recommandée. Au besoin, consulter le responsable du CADRISQ pour d'autres suggestions de techniques de masquage[5].

5. Avant la diffusion des résultats, appliquer l'arrondissement aléatoire aux résultats[6] en utilisant comme base d'arrondissement celle mentionnée au thème J de la section 2, 3 ou 4, selon le cas. Des outils visant à aider l'utilisateur à appliquer un arrondissement aléatoire sont disponibles.

Remarques importantes :

- Il est important de rappeler qu'il faut limiter les sorties intermédiaires[7], car plus leur nombre est élevé, plus les risques de divulgation (par recoupement) augmentent.
- Il est possible que le responsable du CADRISQ doive refuser la diffusion de certains tableaux lorsque ceux-ci sont produits à partir d'une population ou d'une sous-population identifiable[8] qui serait jugée très petite ou très visible ou lorsque le nombre de variables de croisement[9] est trop élevé. En effet, la diffusion de tels tableaux pourrait contrevenir aux obligations de protection des renseignements de l'Institut.
- Une vigilance accrue est de rigueur lorsqu'une étude ou une analyse est faite sur plusieurs années, car le risque de divulgation est plus élevé lorsque l'on croise des variables provenant de périodes différentes. Ce serait le cas par exemple si l'on effectuait le suivi géographique d'un individu (déménagement d'une région à une autre).
- L'Institut a à cœur de se tenir au courant des préoccupations relatives à la protection des renseignements personnels (PRP), et de suivre l'évolution des pratiques et des technologies. Par conséquent, les règles de confidentialité sont susceptibles d'être modifiées. Le responsable du CADRISQ informera l'utilisateur si certaines règles relatives à l'un des ensembles de données dont il se sert venaient à changer.

5. Notons qu'il peut parfois arriver que la diffusion ne soit pas possible.
6. Seules les données contenues dans des tableaux de fréquences doivent être arrondies. Les proportions devront être calculées à partir des fréquences arrondies (numérateur et dénominateur). Certains graphiques, soit ceux qui sont construits à partir d'un tableau de fréquences, tels qu'un histogramme, devront également être construits à partir des fréquences arrondies. Les résultats de modèles ou de tests statistiques n'auront pas à être arrondis.
7. Afin de permettre la consultation avec les pairs des résultats intermédiaires, l'Institut a adopté une approche pour l'accès à distance à des résultats intermédiaires. Consulter le responsable du CADRISQ pour en savoir plus.
8. Consulter la définition de population ou sous-population identifiable dans le glossaire.
9. Consulter la définition de variable de croisement dans le glossaire.

Glossaire

Variable de croisement

Un tableau de fréquences est, en général, formé par le croisement d'une variable d'analyse (synonyme : variable dépendante ou d'intérêt) et d'une variable de croisement (synonyme : variable indépendante ou explicative).

Par exemple, lors de l'analyse de la détresse psychologique selon l'âge, on peut comparer la proportion estimée d'individus se situant à un niveau élevé de l'échelle de détresse psychologique (variable d'analyse) entre les différents groupes d'âge (variable de croisement).

Population ou sous-population identifiable

Une population ou une sous-population est considérée comme identifiable lorsque l'appartenance d'un individu ou d'un regroupement d'individus à celle-ci est soit observable (ex. : handicap physique), soit caractérisée par un environnement particulier (ex. : individus de 65 ans et plus de sexe féminin).

Notons que les notions de variable de croisement et de population (ou sous-population) identifiable sont étroitement liées. En effet, les modalités d'une variable de croisement peuvent, dans certains cas, constituer des populations (ou sous-populations) identifiables.

Cellule vide non structurelle

Une cellule vide est dite non structurelle si elle peut techniquement comporter des individus, mais qu'elle n'en comporte pas. Il ne faut pas confondre ce type de cellule avec la cellule vide structurelle, qui représente une combinaison impossible. Par exemple, « avoir neuf ans » et « avoir trois enfants » sont deux caractéristiques d'une personne qui ne pourraient être combinées. La cellule vide structurelle ne pose pas de problème de confidentialité.

Cellule complète

Une cellule est complète si elle contient la totalité des individus ou un regroupement d'individus, c'est-à-dire 100 % de la somme d'une colonne ou d'une ligne du tableau. Elle peut être structurelle ou non.

Modèle saturé ou presque saturé

Un modèle est saturé ou presque saturé s'il comporte de nombreux coefficients, c'est-à-dire presque autant qu'il y a de combinaisons possibles de valeurs de covariables. Ces modèles peuvent être obtenus lors d'une analyse de variance ou d'une régression.

Index des thèmes

Section 1 – Critère géographique

Critère géographique

Vérifier que la taille de la population de la zone géographique de diffusion pour laquelle des résultats sont produits est d'au moins **1 000** individus[10]. Si ce n'est pas le cas, il faut produire des résultats à un niveau géographique qui respecte ce critère.

La population associée à une zone géographique de diffusion donnée comprend toutes les personnes vivant dans cette zone, et non pas uniquement celles comprises dans le sous-ensemble visé par le projet de recherche. La taille de cette population peut être déterminée à partir des estimations de population basées sur le recensement[11].

Toutefois, si les analyses à effectuer portent sur des travailleurs, la taille de la population doit être établie seulement en fonction des personnes travaillant dans la zone géographique de diffusion. C'est que la distribution géographique des travailleurs n'est pas la même que celle de la population en général. Par ailleurs, s'il s'avère possible de localiser les travailleurs de manière précise à l'intérieur de la zone géographique de diffusion, l'estimation de la taille de la population devrait être basée sur les travailleurs visés par le projet de recherche. Le responsable du CADRISQ peut, au besoin, accompagner l'utilisateur dans la détermination de la population dont la taille doit être estimée.

10. Dans certaines situations, il se peut que le seuil du critère géographique à appliquer soit plus élevé. Ce seuil dépend, entre autres, des informations contenues dans la banque de données administratives.
11. Pour déterminer cette taille, consulter le site Web de Statistique Canada ou de l'Institut de la statistique du Québec, afin d'accéder aux plus récentes données, selon la ventilation souhaitée (âge, sexe, découpage géographique, etc.).

Section 2 – Règles de confidentialité STANDARD

Résultats produits aux CADRISQ ou en accès à distance à partir d'un fichier de données administratives

A Thème : Cellule à faible fréquence

Règle : Toutes les statistiques d'un tableau de résultats destinées à être diffusées doivent être basées sur au moins **cinq** individus[12]. Dans le cas d'une estimation de proportion, il doit y avoir au moins **cinq** individus au numérateur. C'est dire que toutes les cellules du tableau de fréquences correspondant doivent contenir au moins cinq individus. Si ce n'est pas le cas, un masquage doit être appliqué (ex. : regroupement des modalités problématiques). Notons que cette règle ne s'applique pas dans le cas des cellules vides. Pour ces dernières, il faut appliquer la règle **C**.

B Thème : Cellule complète

Règle : La diffusion d'un résultat issu d'une cellule complète ne peut se faire, à moins qu'il ne provienne d'une cellule complète structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule complète non structurelle dans le tableau.

C Thème : Cellule vide

Règle : La diffusion d'un résultat issu d'une cellule vide ne peut se faire, à moins qu'il ne provienne d'une cellule vide structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule vide non structurelle dans le tableau.

D Thème : L'étendue et la valeur minimale ou maximale

Règle : L'étendue et la valeur minimale ou maximale de certaines variables comme l'âge, le poids, le revenu ou la taille du ménage ne doivent pas être diffusées. Afin d'illustrer la dispersion des valeurs, il faut plutôt utiliser une statistique comme l'écart-type.

E Thème : Statistique individuelle telle qu'une moyenne ou un total

Règle : Toute statistique individuelle produite (ex. : moyenne ou total d'une variable continue) doit se fonder sur au moins **cinq** individus[12]. Une statistique produite à partir de moins de cinq individus doit être recalculée selon un domaine contenant plus d'individus.

F Thème : Statistique du ratio

Règle : Un ratio ne peut être diffusé si l'une de ses composantes (numérateur ou dénominateur) ne peut être diffusée. Le cas échéant, le ratio doit être recalculé selon un domaine contenant plus d'individus.

G Thème : Statistique d'ordre telle que la médiane et le centile

Règle : On doit trouver au moins **cinq** individus[12] au-dessus et au moins **cinq** individus au-dessous de ces statistiques d'ordre. Si ce n'est pas le cas, d'autres statistiques d'ordre doivent être calculées.

H Thème : Modèle saturé ou presque saturé

Règle : Les résultats provenant d'un modèle saturé ou presque saturé, qu'ils soient obtenus par exemple lors d'une analyse de variance ou d'une régression, ne doivent pas être diffusés.

I Thème : Nuage de points, courbe de survie, graphique de résidus ou graphique en boîte

Règle : La diffusion de tels graphiques doit être faite avec circonspection puisque ceux-ci affichent des valeurs qui s'appliquent à des individus particuliers. Les graphiques comportant des valeurs extrêmes ne devraient pas être diffusés.

J Thème : Arrondissement aléatoire des fréquences

Règle : Toutes les fréquences issues de données administratives doivent être arrondies aléatoirement en base **5**, et on doit s'assurer que les proportions sont calculées à partir de ces fréquences arrondies.

12. La définition d'un individu est ici soit un individu seul, soit un regroupement d'individus.

Section 3 – Règles de confidentialité STANDARD-10

Résultats produits aux CADRISQ ou en accès à distance à partir d'un fichier de données administratives

A **Thème : Cellule à faible fréquence**

Règle : Toutes les statistiques d'un tableau de résultats destinées à être diffusées doivent être basées sur au moins **10** individus[13]. Dans le cas d'une estimation de proportion, il doit y avoir au moins **10** individus au numérateur. C'est dire que toutes les cellules du tableau de fréquences correspondant doivent contenir au moins 10 individus. Si ce n'est pas le cas, un masquage doit être appliqué (ex. : regroupement des modalités problématiques). Notons que cette règle ne s'applique pas dans le cas des cellules vides. Pour ces dernières, il faut appliquer la règle **C**.

B **Thème : Cellule complète**

Règle : La diffusion d'un résultat issu d'une cellule complète ne peut se faire, à moins qu'il ne provienne d'une cellule complète structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule complète non structurelle dans le tableau.

C **Thème : Cellule vide**

Règle : La diffusion d'un résultat issu d'une cellule vide ne peut se faire, à moins qu'il ne provienne d'une cellule vide structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule vide non structurelle dans le tableau.

D **Thème : L'étendue et la valeur minimale ou maximale**

Règle : L'étendue et la valeur minimale ou maximale de certaines variables comme l'âge, le poids, le revenu ou la taille du ménage ne doivent pas être diffusées. Afin d'illustrer la dispersion des valeurs, il faut plutôt utiliser une statistique comme l'écart-type.

E **Thème : Statistique individuelle telle qu'une moyenne ou un total**

Règle : Toute statistique individuelle produite (ex. : moyenne ou total d'une variable continue) doit se fonder sur au moins **10** individus[13]. Une statistique produite à partir de moins de 10 individus doit être recalculée selon un domaine contenant plus d'individus.

F **Thème : Statistique du ratio**

Règle : Un ratio ne peut être diffusé si l'une de ses composantes (numérateur ou dénominateur) ne peut être diffusée. Le cas échéant, le ratio doit être recalculé selon un domaine contenant plus d'individus.

G **Thème : Statistique d'ordre telle que la médiane et le centile**

Règle : On doit trouver au moins **10** individus[13] au-dessus et au moins **10** individus au-dessous de ces statistiques d'ordre. Si ce n'est pas le cas, d'autres statistiques d'ordre doivent être calculées.

H **Thème : Modèle saturé ou presque saturé**

Règle : Les résultats provenant d'un modèle saturé ou presque saturé, qu'ils soient obtenus par exemple lors d'une analyse de variance ou d'une régression, ne doivent pas être diffusés.

I **Thème : Nuage de points, courbe de survie, graphique de résidus ou graphique en boîte**

Règle : La diffusion de tels graphiques doit être faite avec circonspection puisque ceux-ci affichent des valeurs qui s'appliquent à des individus particuliers. Les graphiques comportant des valeurs extrêmes ne devraient pas être diffusés.

J **Thème : Arrondissement aléatoire des fréquences**

Règle : Toutes les fréquences issues de données administratives doivent être arrondies aléatoirement en base **5**, et on doit s'assurer que les proportions sont calculées à partir de ces fréquences arrondies.

13. La définition d'un individu est ici soit un individu seul, soit un regroupement d'individus.

Section 4 – Règles de confidentialité STANDARD-15

Résultats produits aux CADRISQ ou en accès à distance à partir d'un fichier de données administratives

A **Thème : Cellule à faible fréquence**

Règle : Toutes les statistiques d'un tableau de résultats destinées à être diffusées doivent être basées sur au moins **15** individus[14]. Dans le cas d'une estimation de proportion, il doit y avoir au moins **15** individus au numérateur. C'est dire que toutes les cellules du tableau de fréquences correspondant doivent contenir au moins 15 individus. Si ce n'est pas le cas, un masquage doit être appliqué (ex. : regroupement des modalités problématiques). Notons que cette règle ne s'applique pas dans le cas des cellules vides. Pour ces dernières, il faut appliquer la règle **C**.

B **Thème : Cellule complète**

Règle : La diffusion d'un résultat issu d'une cellule complète ne peut se faire, à moins qu'il ne provienne d'une cellule complète structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule complète non structurelle dans le tableau.

C **Thème : Cellule vide**

Règle : La diffusion d'un résultat issu d'une cellule vide ne peut se faire, à moins qu'il ne provienne d'une cellule vide structurelle. Il faut penser à un regroupement des modalités de façon à ce qu'il n'y ait plus de cellule vide non structurelle dans le tableau.

D **Thème : L'étendue et la valeur minimale ou maximale**

Règle : L'étendue et la valeur minimale ou maximale de certaines variables comme l'âge, le poids, le revenu ou la taille du ménage ne doivent pas être diffusées. Afin d'illustrer la dispersion des valeurs, il faut plutôt utiliser une statistique comme l'écart-type.

E **Thème : Statistique individuelle telle qu'une moyenne ou un total**

Règle : Toute statistique individuelle produite (ex. : moyenne ou total d'une variable continue) doit se fonder sur au moins **15** individus[14]. Une statistique produite à partir de moins de 15 individus doit être recalculée selon un domaine contenant plus d'individus.

F **Thème : Statistique du ratio**

Règle : Un ratio ne peut être diffusé si l'une de ses composantes (numérateur ou dénominateur) ne peut être diffusée. Le cas échéant, le ratio doit être recalculé selon un domaine contenant plus d'individus.

G **Thème : Statistique d'ordre telle que la médiane et le centile**

Règle : On doit trouver au moins **15** individus[14] au-dessus et au moins **15** individus au-dessous de ces statistiques d'ordre. Si ce n'est pas le cas, d'autres statistiques d'ordre doivent être calculées.

H **Thème : Modèle saturé ou presque saturé**

Règle : Les résultats provenant d'un modèle saturé ou presque saturé, qu'ils soient obtenus par exemple lors d'une analyse de variance ou d'une régression, ne doivent pas être diffusés.

I **Thème : Nuage de points, courbe de survie, graphique de résidus ou graphique en boîte**

Règle : La diffusion de tels graphiques doit être faite avec circonspection puisque ceux-ci affichent des valeurs qui s'appliquent à des individus particuliers. Les graphiques comportant des valeurs extrêmes ne devraient pas être diffusés.

J **Thème : Arrondissement aléatoire des fréquences**

Règle : Toutes les fréquences issues de données administratives doivent être arrondies aléatoirement en base **5**, et on doit s'assurer que les proportions sont calculées à partir de ces fréquences arrondies.

14. La définition d'un individu est ici soit un individu seul, soit un regroupement d'individus.

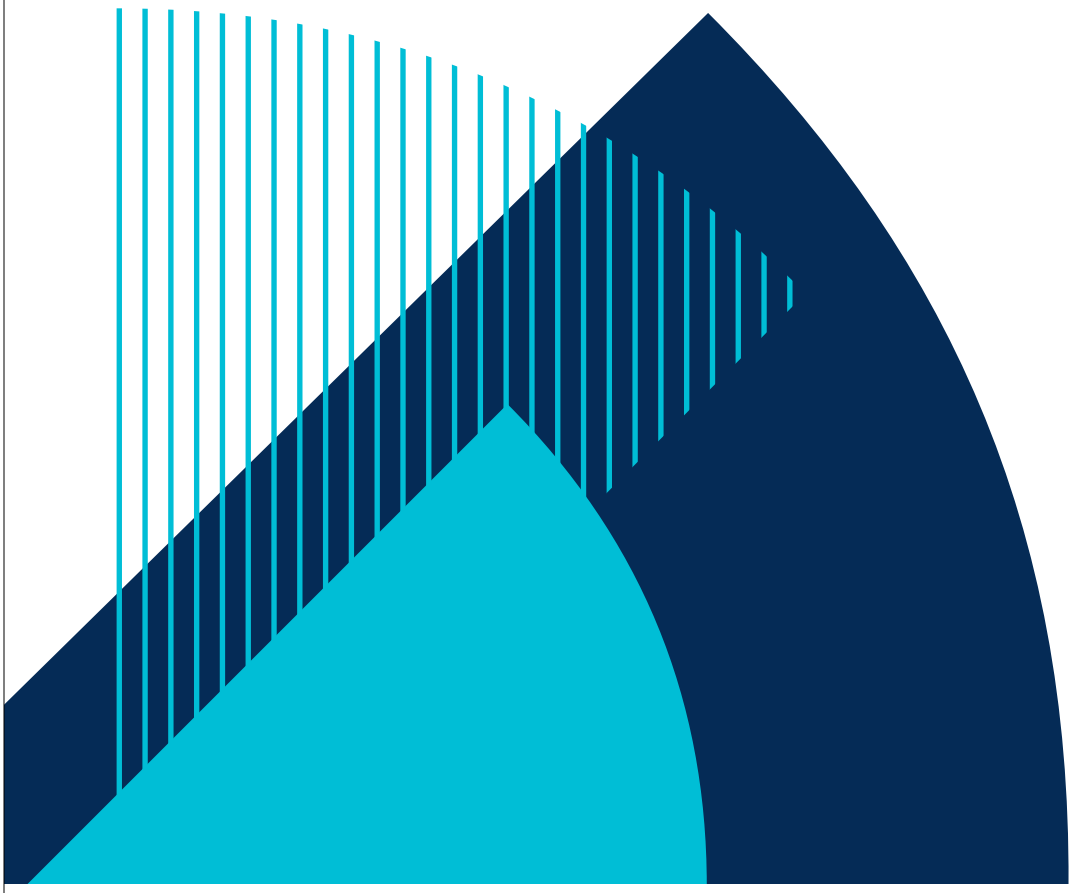
« La statistique au
service de la société :
la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec

Annexe 3

Politique de sécurité de l'information



INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Note

La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes.

Date d'approbation :	2017-05-16
Responsable de la mise à jour :	Responsable organisationnel de la sécurité de l'information (ROSI)
Dernière mise à jour :	Février 2022

Table des matières

1 Préambule

L'Institut de la statistique du Québec (ISQ) mise sur une solide culture de la confidentialité. 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.

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'articulent à l'intérieur d'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 principaux acteurs.

2 Définitions

Actif informationnel

Un actif informationnel peut être une information, quel que soit son support (papier, support électronique, etc.) ou son canal de communication (téléphone, télécopie, voix, etc.) ou encore l'actif peut être 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.

Confidentialité

Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information

L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par 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.

Disponibilité

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

Intégrité

Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

3 Cadre légal et administratif

La politique de sécurité de l'information s'inscrit principalement dans un contexte régi par la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03) qui établit les règles de gouvernance et de gestion en matière de ressources informationnelles.

En janvier 2014, le gouvernement a adopté, par décret, plusieurs documents en vertu de cette loi, notamment :

- la Directive sur la sécurité de l'information gouvernementale ; CT-11-2-2-2, 23 janvier 2014 ;
- le Cadre gouvernemental de gestion de la sécurité de l'information ; Secrétariat du Conseil du trésor, édition 2014 ;
- le Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information ; Secrétariat du Conseil du trésor, édition 2014 ;

Ces documents déterminent les rôles et responsabilités des intervenants gouvernementaux et les obligations des organismes publics, notamment pour adopter et 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*.

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 son support ou son moyen de communication.

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

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

- assurer, tout au long du cycle de vie de l'information, les différentes propriétés d'une information : disponibilité, intégrité et confidentialité (DIC) ;
- atteindre un degré adéquat de sécurité de l'information par une compréhension commune et l'engagement constant de tous les utilisateurs, ainsi que de ses partenaires et fournisseurs ;
- soutenir toutes les activités de l'ISQ avec une démarche globale de gestion des risques et des incidents de sécurité ;
- 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, quelle que soit sa forme, 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, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, 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 avoir accès.

L'information ou 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.

À titre d'exemple, ceux :

- obtenus en vertu de la Loi sur l'Institut de la statistique du Québec ;
- utilisés dans 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. Chaque acteur est imputable en regard du bon usage des informations dans le cadre de ses 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. 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, à garantir l'intégrité et à assurer 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 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 à :

- assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée ;
- 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, assurant ainsi une stricte confidentialité ;
- permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif ;
- se prémunir 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 l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion interne de la sécurité permettant une reddition claire de l'imputabilité.

6.4 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, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

6.5 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. Pour les prochaines années, elles visent à :

- Renforcer la gouvernance de la sécurité :
  - s'assurer 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 ;
  - s'assurer minimalement de la réalisation d'audits de sécurité de l'information ou de tests d'intrusion et de vulnérabilité à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information ;
  - s'assurer que les ententes de service et les contrats, conclus avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information.
- Formaliser des pratiques en s'assurant de la mise en œuvre de processus qui permettent d'assurer :
  - la gestion des risques de sécurité de l'information dès le début d'un projet qu'ils soient informatisés ou non, en s'appuyant sur une catégorisation officielle de l'information ;
  - la gestion des accès à l'information et la gestion des incidents.
- Développer et maintenir des compétences clés en la matière :
  - sensibiliser et former tous les utilisateurs en fonction de leurs profils et des enjeux de sécurité de l'information.

8 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.

- **Le directeur général** est le premier responsable de la protection et de la sécurité de l'information ainsi que de la gouvernance de ces aspects. Il nomme un responsable organisationnel de la sécurité de l'information qui voit à la mise en œuvre de cette politique. Il désigne les membres du Comité de gouvernance de la sécurité de l'information et statue sur les avis et recommandations du même comité. Il désigne également les détenteurs de l'information. Enfin, il approuve le plan d'action en matière de sécurité et autorise les budgets correspondants.
- **Le responsable organisationnel de la sécurité de l'information** (ROSI) représente l'ISQ auprès du dirigeant principal de l'information (DPI) et il relaie les orientations et les priorités d'intervention gouvernementales en ce qui regarde la sécurité de l'information. Il assiste le directeur général 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. En outre, il assure la coordination et la cohérence des actions de sécurité de l'information menées à l'ISQ par les différents acteurs et il établit les partenariats internes à ces fins.
- **Le conseiller organisationnel en sécurité de l'information** (COSI), au-delà de son rôle de soutien auprès du ROSI, il est notamment chargé d'assister les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information. De plus, il joue un rôle dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information.
- **Le coordonnateur organisationnel de la gestion des incidents** (COGI) voit à la mise en œuvre du processus de la gestion des incidents de sécurité de l'information à l'ISQ. Il participe en outre au réseau d'alerte gouvernemental.
- **Le détenteur de l'information** a la responsabilité de veiller à la mise en place et à l'application des mesures de sécurité propres 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 de l'information a la responsabilité de catégoriser l'information relevant de sa responsabilité selon sa valeur au niveau de la disponibilité, de l'intégrité et de la confidentialité.

- **Le responsable de la gestion des technologies** a la responsabilité de mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique. Il 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 responsable de la sécurité physique** met en place les mesures de protection physique des actifs informationnels, des biens et des locaux.
- **Le gestionnaire** est responsable, auprès du personnel relevant de son autorité, de la mise en œuvre des dispositions de la présente politique en veillant à ce que ses employés utilisent correctement les actifs informationnels. Il 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 gestionnaire est le premier responsable de la sensibilisation de ses employés. Il veille à ce que les employés sous sa gouverne utilisent correctement les actifs informationnels. Il 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*, en complément à la présente politique.

9 Obligations des utilisateurs

Tout utilisateur a l'obligation de protéger les informations et les actifs mis à sa disposition par l'ISQ. À cette fin, il doit :

- prendre connaissance de la présente politique y adhérer ;
- utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition 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 à son gestionnaire tout acte dont il a connaissance, 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 confirme à l'ouverture d'un poste de travail de l'ISQ qu'il s'engage à respecter les modalités de la politique de sécurité de l'information et il confirme qu'il comprend que des sanctions peuvent être imposées s'il y contrevient ;
- au moment de son départ de l'ISQ, 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.

10 Sanctions

Des vérifications et des enquêtes internes sont réalisées à la demande du directeur général pour vérifier le respect de la présente politique ou des directives en découlant. Lorsqu'un utilisateur y contrevient, il s'expose à des mesures disciplinaires, administratives ou légales.

11 Dispositions finales

- Le directeur général approuve la présente politique.
- Le responsable organisationnel de la sécurité de l'information 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 de complément 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 directeur général.

2017-05-16	
Date approbation	Stéphane Mercier, directeur général

« La statistique au
service de la société :
la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec

Annexe 4

f

INSTITUT
DE LA STATISTIQUE
DU QUÉBEC

Politique de sécurisation des locaux

Québec

Note
La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes.

Date d'approbation :	18 juin 2003
Unité responsable de la mise à jour :	Direction des ressources financières et matérielles
Dernière mise à jour :	26 février 2019

TABLE DES MATIÈRES

DÉFINITIONS

Carte d'accès :	Carte à puce servant à ouvrir une porte verrouillée dans les immeubles occupés par l'Institut de la statistique du Québec (Institut).
Clé :	Pièce métallique permettant de verrouiller et de déverrouiller une ou des serrures.
Pastille :	Puce électronique accolée à la carte d'accès de l'Institut permettant d'ouvrir les portes de l'immeuble en dehors des heures de bureau.
Permis de circuler :	Carte donnant droit à son titulaire de circuler dans les locaux de l'Institut. Il existe deux types de permis de circuler :
• Carte d'identité :	Carte avec photo ou sans photo permettant à son titulaire de se déplacer seul dans les locaux de l'Institut;
• Carte visiteur :	Carte sans photo obligeant son titulaire à être en tout temps accompagné d'un membre du personnel pour pouvoir se déplacer dans les locaux de l'Institut.
Personnel :	Le personnel est constitué de :
• Employé de l'Institut :	Employé de l'une des catégories d'emploi de la fonction publique (étudiant, stagiaire, fonctionnaire, professionnel ou gestionnaire) ayant un statut d'emploi occasionnel, temporaire ou permanent à l'Institut, ceci inclut également le statut de prêt de service;
• Employé contractuel :	Employé d'une firme externe engagé à contrat;
• Employé d'entretien et agent de sécurité :	Employé d'une entreprise ayant un lien contractuel direct ou indirect avec l'Institut pour fournir un service ou un produit qui n'est pas en lien direct avec la mission de l'Institut.
Visiteur :	Personne qui ne fait pas partie du personnel et qui est en visite dans les locaux de l'Institut.

POLITIQUE DE SÉCURISATION DES LOCAUX

Le présent document édicte les règles et précise les responsabilités de chacun au regard du contrôle d'accès aux locaux de l'Institut. Il indique les lignes directrices à suivre pour que la sécurité physique et environnementale des locaux de l'Institut soient assurées en tout temps. Même si de nombreux moyens administratifs, mécaniques et électroniques concourent à l'atteinte de cet objectif, la vigilance et la collaboration du personnel demeurent essentielles.

1. INTRODUCTION

Cette politique intègre les meilleures pratiques reconnues en matière de sécurité. En effet, comme l'Institut détient, manipule et gère des données confidentielles, il est impératif qu'il soit en mesure de les protéger contre toute intrusion.

2. CHAMP D'APPLICATION

Cette politique concerne toute personne qui accède aux locaux de l'Institut.

3. LIGNES DIRECTRICES

- Tout droit d'accès à un local de l'Institut doit être justifié selon les besoins de la fonction du membre du personnel;
- Les dispositifs de contrôle d'accès aux locaux doivent être adaptés au niveau de risque et de préjudice associé à la divulgation de l'information confidentielle;
- Toute personne qui circule dans les locaux de l'Institut doit porter en tout temps et de façon visible la carte d'identité ou la carte visiteur qui lui a été remise.

4. RÔLES ET RESPONSABILITÉS

4.1. Directeur général

Le directeur général est le premier responsable pour toute question de sécurité à l'Institut. De plus, il doit :

- Approuver les demandes d'accès des chercheurs aux Centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ) par la signature d'un contrat de recherche.

4.2. Gestionnaires

- Veiller à ce que le personnel relié à leur direction respecte l'affectation des différentes zones restreintes;

- En collaboration avec le Responsable de la sécurité physique (RSP) :
  - Attribuer les droits d'accès aux membres du personnel reliés à leur direction selon les besoins inhérents à la fonction de ceux-ci et des zones dont ils sont responsables;
  - Faire une révision complète et mettre à jour les droits d'accès du personnel relié à leur direction annuellement;
  - Valider les rapports d'entrées-sorties et les registres d'événements au besoin.
- Reprendre la carte d'identité et la carte d'accès du membre du personnel relié à leur direction quand la date de validité est expirée, qu'il y a fin d'emploi avec l'Institut ou à la demande du RSP, et les remettre au RSP;
- Aviser le RSP de toute situation susceptible de porter atteinte à la sécurité.

4.3. Responsable de la sécurité physique (RSP)[1]

Le RSP assume la sécurité physique et environnementale des locaux de l'Institut. Il exerce, entre autres, les tâches suivantes :

- Mettre à jour et appliquer cette politique;
- Assurer l'harmonisation de cette politique avec les règles d'accès aux immeubles occupés par l'Institut en collaborant avec les autres intervenants associés à ces immeubles;
- Administrer les cartes d'identité, les cartes d'accès, les pastilles et les clés (émission, révocation, vérification, etc.);
- Reprendre la carte d'identité du personnel lorsqu'une nouvelle est émise;
- Fournir aux gestionnaires annuellement une liste des droits d'accès du personnel relié à leurs directions;
- Administrer le matériel de sécurité physique (maintenance, supervision et alertes);
- Faire le suivi des registres d'accès aux locaux;
- Effectuer de façon ad hoc des vérifications de conformité d'accès dans les locaux;
- S'assurer de la mise au rebut sécuritaire des supports de l'information;
- Élaborer, mettre à jour et appliquer des directives, des guides et des procédures propres à son domaine d'intervention;
- Informer le Coordonnateur organisationnel de gestion des incidents (COGI) de tout incident ou risque d'incident;
- Apporter les modifications qui s'imposent après un incident ou la découverte d'un risque d'incident;
- Faire de la sensibilisation et des actions préventives;
- Assurer la veille dans le domaine;
- Faire annuellement une révision complète et mettre à jour les droits d'accès des employés d'entretien et des agents de sécurité.

Le RSP se réserve le droit de révoquer, de refuser ou de limiter l'accès aux locaux en fonction des besoins de sécurité ou s'il n'est pas en adéquation avec les besoins du requérant.

1. Les désignations du RSP et du COGI sont disponibles dans la section Sécurité de l'information/Responsabilités de l'intranet.

4.4. Coordonnateur organisationnel de gestion des incidents (COGI)[1]

- Contribuer aux analyses de risques;
- Participer à la coordination des actions aux incidents et des stratégies de réaction appropriées, lorsque requise ;
- Peut vérifier les accès de quiconque sans préavis et de façon ad hoc en raison de son rôle de surveillance.

4.5. Comité de gouvernance de la sécurité de l'information (CGSI)

- Examiner et entériner les recommandations concernant notamment la politique, les orientations et les moyens de contrôle relatifs à la sécurisation des locaux;
- Entériner les solutions recommandées visant à corriger ou améliorer la sécurité physique et environnementale lorsque la situation l'exige.

4.6. Préposés à l'accueil

- Accueillir les visiteurs;
- Administrer les cartes d'identité temporaires, les cartes d'accès temporaires, les pastilles temporaires et les cartes visiteurs;
- Tenir à jour le registre des visiteurs;
- Tenir à jour les registres des cartes d'identité temporaires, des cartes d'accès temporaires et des pastilles temporaires.

4.7. Responsables des Centres d'accès aux données de recherche de l'Institut de la statistique du Québec (CADRISQ)

- Traiter les demandes d'accès à un CADRISQ;
- Mettre en œuvre la *Procédure pour l'accueil d'un nouveau chercheur au CADRISQ*;
- Administrer les cartes d'identité et les cartes d'accès des chercheurs, au besoin en collaboration avec le RSP;
- Remettre le *Guide à l'intention des chercheurs exploitant des données au CADRISQ* aux chercheurs et s'assurer de sa mise en œuvre;
- Tenir à jour le registre quotidien de présence;
- Reprendre la carte d'identité et la carte d'accès du chercheur à la fin du contrat et les remettre au RSP, le cas échéant;
- Aviser le RSP de tout incident ou risque d'incident en lien avec les locaux des CADRISQ;
- Effectuer de façon ad hoc des vérifications de conformité d'accès dans les locaux des CADRISQ.

4.8. Membres du personnel

- Porter sa carte d'identité bien en évidence pour circuler dans les locaux;
- Protéger sa carte et la conserver dans un lieu sûr en dehors des locaux de l'ISQ;
- Ne pas prêter, transférer, emprunter ou altérer une carte d'identité ou une carte d'accès;

1. Les désignations du RSP et du COGI sont disponibles dans la section Sécurité de l'information/Responsabilités de l'intranet.

- Déclarer au RSP immédiatement la perte ou le vol de sa carte d'identité, de sa carte d'accès ou de sa pastille pour que celui-ci puisse la désactiver sans tarder;
- Questionner toute personne qui n'affiche pas de carte d'identité ou tout visiteur non accompagné;
- Aviser le RSP de tout écart aux directives de sécurité;
- Ne pas pénétrer dans une zone à accès contrôlé ou de sécurité à moins que le responsable de cette zone ne l'y autorise;
- Aviser ses visiteurs qu'ils doivent s'identifier au poste d'accueil avant d'accéder aux locaux;
- Assumer la responsabilité du comportement de ses visiteurs;
- Lors du départ d'un visiteur, l'accompagner jusqu'à une zone externe et s'assurer que la carte visiteur est retournée;
- Lors d'une visite en dehors des heures de bureau, le membre du personnel doit suivre la procédure décrite au point 7.4.2;
- Lorsqu'une nouvelle carte d'identité lui est émise, remettre la carte d'identité expirée au RSP;
- Lorsqu'il y a fin d'emploi, remettre sa carte d'identité et sa carte d'accès à son gestionnaire responsable.

4.9. Agents de sécurité

- Effectuer une ronde journalière dans les locaux de l'Institut à Québec;
- Aviser le RSP de tout incident ou risque d'incident.

5. ZONAGE

Les diverses zones regroupent les locaux dont les besoins d'accès et de la fonction sont les mêmes. Le niveau de sécurité de chacune des zones est déterminé par ce qu'elle contient, c'est-à-dire en fonction du niveau de risque et de préjudice associés à la divulgation d'informations confidentielles.

5.1. Zone externe

L'Institut n'est pas responsable de la zone externe qui est accessible au public en tout temps. Elle est située à l'extérieur des locaux de l'Institut.

Exemples : corridors, ascenseurs, toilettes.

5.2. Zone publique

La zone publique se trouve à l'intérieur des locaux de l'Institut et celui-ci en est responsable. C'est le seul endroit où les visiteurs peuvent se déplacer sans être accompagnés d'un membre du personnel.

Exemples : postes d'accueil de l'Institut, salle Zéphirin-Bérubé à Québec, salles de réunions 5a, 5b, 5c, 5d et 10a à Montréal.

5.3. Zone de travail

La zone de travail est confiée à une ou plusieurs directions de l'Institut et tout le personnel y a accès durant les heures de bureau dans leur territoire habituel de travail.

Les directions qui partagent la même zone de travail sont conjointement responsables de cette zone. Les gestionnaires doivent gérer les droits d'accès des membres du personnel associés à leur direction selon les besoins reliés à leur fonction. Chaque gestionnaire est responsable de déterminer le risque occasionné par le partage d'une zone de travail avec les autres directions. Le gestionnaire qui accorde un droit d'accès à une zone partagée doit tenir compte du risque et du préjudice encourus par les autres directions qui la partagent.

Exemple : espace de travail des employés de l'Institut.

5.4. Zone de travail à accès contrôlé

La zone de travail à accès contrôlé correspond à un espace physique qui ne doit pas être accessible à tout le personnel, le plus souvent parce qu'on y trouve des renseignements personnels et confidentiels. En dehors des heures de bureau, tout document de cet ordre doit être rangé dans un classeur verrouillé. Seul le personnel autorisé par leur gestionnaire responsable et le gestionnaire de ladite zone peut circuler dans cette zone.

Exemples : ateliers informatiques, salle CATI, bureau des gestionnaires.

5.5. Zone sécurisée

La zone sécurisée correspond à un espace physique où peu d'individus peuvent avoir accès parce qu'il s'y trouve des renseignements dont la divulgation aurait des conséquences graves. Généralement, cette zone est sous la responsabilité d'une seule direction. Seul le personnel autorisé par leur gestionnaire responsable et le gestionnaire de ladite zone peut y circuler. En d'autres termes, la zone entière doit être protégée, et pas seulement son accès.

Exemples : centres de traitement informatique principal et auxiliaire, locaux de télécommunication, salles 3.25a et 3.25b, CADRISQ.

6. CONTRÔLE D'ACCÈS DES ZONES

Le contrôle d'accès entre les zones est effectué autant que possible à l'aide de moyens électroniques. Chaque membre du personnel possède une carte d'accès unique qui l'identifie et qui lui donne accès aux zones correspondant à leur niveau d'accès autorisé par leur gestionnaire responsable.

Pour les zones ayant un niveau de sécurité plus élevé, le nombre de personnes qui ont accès à ces zones doit être limité autant que possible et chaque accès doit être justifié.

Pour les zones dont le niveau de sécurité est plus bas, il est possible d'installer une serrure dont l'efficacité est reconnue.

Tout employé de l'Institut a accès aux zones publiques et à sa zone de travail du lundi au vendredi de 6 h à 24 h ainsi qu'aux autres zones entre 7 h 30 et 18 h.

L'accès à l'immeuble situé au 200, chemin Sainte-Foy à Québec peut se faire seulement entre 7 h et 18 h, tandis que pour celui situé au 1200, avenue McGill College à Montréal, l'accès peut se faire entre 6 h et 19 h. Tout accès à l'immeuble du territoire habituel de travail du membre du personnel en dehors de ces heures doit être autorisé par son gestionnaire responsable.

L'accès aux CADRISQ se fait durant les heures de bureau, soit de 8 h 30 à 12 h et de 13 h à 16 h 30.

Certains niveaux de sécurité dépendent de la fonction occupée par le membre du personnel. Tout accès à une zone autre que celle définie pour son travail régulier doit être autorisé par le gestionnaire responsable de ladite zone.

7. MODALITÉS D'APPLICATION

7.1. Circulation dans les locaux de l'Institut

Toute personne qui circule dans les locaux de l'Institut doit porter en évidence son permis de circuler, exception faite pour les chercheurs ayant seulement accès à un CADRISQ autre que celui situé au 200, chemin Sainte-Foy à Québec. Il existe deux types de permis de circuler :

7.1.1. Carte d'identité

Il existe deux types de cartes d'identité :

- la carte d'identité **régulière (a)** : carte d'identité avec photo remise systématiquement dès l'arrivée d'un nouveau membre du personnel ou lors du renouvellement d'une carte expirée;
- la carte d'identité **temporaire (b)** : carte d'identité sans photo remise au membre du personnel lorsqu'il oublie sa carte d'identité ou sa carte d'accès, ou lors de la demande temporaire d'une pastille.

À l'endos de toutes les cartes d'identité, on retrouve le libellé suivant :

« Cette carte est la propriété de l'Institut de la statistique du Québec
et doit être rendue sur demande ou au moment du départ.
Autorisée par : le directeur général »

a) Carte d'identité régulière :

Chaque carte d'identité régulière est reliée à une carte d'accès comportant un numéro unique qui correspond à une entrée dans le logiciel de gestion de la sécurité. Ces cartes comportent les caractéristiques suivantes :

- la carte est bleue pour les employés de l'Institut;
- la carte est verte pour les employés contractuels, les employés d'entretien et les agents de sécurité;
- l'identification visuelle de l'Institut;
- la photo du détenteur;

- le nom et le prénom du détenteur;
- les mots « Valide jusqu'au », suivi de la date d'expiration;
- le nom de l'entreprise (carte verte seulement).

b) Carte d'identité temporaire :

Chaque carte d'identité temporaire comporte un numéro unique qui correspond à une entrée dans le registre des cartes d'identité temporaires et des cartes d'accès temporaires ou dans le registre des pastilles temporaires. Il existe trois types de cartes d'identité temporaires :

Couleur de la carte :	Bleu	Orange	Turquoise
Utilisée en cas :	d'oubli de sa carte d'identité ou de sa carte d'accès	d'oubli de sa carte d'identité ou de sa carte d'accès qui est reliée à une pastille	de demande temporaire d'une pastille
Identification visuelle de l'Institut :	oui	oui	non
Mention indiquée :	« Carte temporaire »	« Carte temporaire avec puce »	« Carte à puce »
Numéro unique de :	4 chiffres	4 chiffres	1 à 10

7.1.2. Carte visiteur

Chaque carte visiteur comporte un numéro unique de 4 chiffres qui correspond à une entrée dans le registre des visiteurs. Spécifiquement pour les visiteurs allant à la salle Zéphirin-Bérubé à Québec, une carte d'accès pouvant ouvrir la porte vitrée du 5e étage est remise en même temps que la carte visiteur. Ces cartes contiennent :

- la carte est blanche;
- l'identification visuelle de l'Institut;
- la mention « Visiteur »;
- le numéro de la carte visiteur.

7.1.3. Carte d'accès

À la suite de l'assermentation du nouveau membre du personnel via le *Modèle d'engagement à la confidentialité applicable aux membres du personnel de l'Institut de la statistique du Québec,* ou le *Modèle d'engagement à la confidentialité applicable aux contractants* le cas échéant, dans lequel il s'engage à respecter cette politique, une carte d'accès lui est remise. Chaque carte d'accès a un numéro unique qui correspond à une entrée dans le logiciel de gestion de la sécurité. Les informations suivantes y sont requises :

- le numéro de la carte d'accès;
- le nom et le prénom du détenteur;
- le nom de la direction ou de l'organisme auquel le détenteur est rattaché;
- le niveau d'accès;
- la date d'expiration;
- le statut de la carte (valide ou expiré).

7.1.4. Oubli d'une carte d'identité, d'une carte d'accès ou d'une pastille

Le membre du personnel qui oublie sa carte d'identité, sa carte d'accès ou sa carte d'accès avec pastille doit se rendre à l'accueil de l'Institut où le préposé à l'accueil lui remettra une ou des cartes temporaires le cas échéant. Ces cartes possèdent les mêmes caractéristiques que les cartes régulières, sauf que les privilèges d'accès sont limités à 24 heures. Les cartes temporaires doivent être retournées au poste d'accueil dès leur expiration.

7.1.5. Registre des cartes d'identité temporaires et des cartes d'accès temporaires

Le registre des cartes d'identité temporaires et des cartes d'accès temporaires contient les informations suivantes :

- le numéro de la carte d'identité temporaire;
- le numéro de la carte d'accès temporaire, le cas échéant;
- le numéro de la pastille temporaire, le cas échéant;
- le nom, le prénom et la direction du membre du personnel qui emprunte la ou les cartes;
- la signature dudit membre;
- la date d'emprunt de la ou des cartes temporaires;
- une section commentaire.

7.1.6. Perte d'une carte d'identité, d'une carte d'accès ou d'une pastille

Le membre du personnel qui perd l'une de ses cartes doit en aviser immédiatement le RSP qui en émettra une nouvelle après avoir désactivé celle perdue. Le RSP vérifiera s'il y a eu utilisation de ladite carte depuis l'incident et, dans l'affirmative, en avisera le COGI.

7.2. Circulation des employés contractuels, des employés d'entretien et des agents de sécurité

À la suite de leur assermentation, les employés contractuels, les employés d'entretien et les agents de sécurité obtiennent une carte d'identité de couleur verte et une carte d'accès. Ces cartes leur permettent de circuler librement au même titre que les employés de l'Institut selon le niveau d'accès attribué par leur gestionnaire responsable.

7.3. Circulation des visiteurs

Tous les visiteurs doivent se présenter au poste d'accueil de l'Institut pour s'enregistrer durant les heures de bureau. La carte visiteur reçue à l'accueil doit être portée bien en vue, et en permanence, pour circuler dans les locaux de l'Institut. Le détenteur de cette carte doit être accompagné en tout temps par un membre du personnel dans les zones de travail, de travail à accès contrôlé et de sécurité.

7.3.1. Registre des visiteurs

Une inscription dans le registre des visiteurs, situé au poste d'accueil de l'Institut, doit être faite pour chaque visiteur. Ce registre contient les renseignements suivants :

- la date de la visite;

- le nom et le prénom du visiteur;
- la signature du visiteur;
- le nom et le prénom du membre du personnel qui prend le visiteur en charge;
- l'heure d'arrivée du visiteur;
- l'heure de départ du visiteur;
- le numéro de la carte visiteur.

Pour le Centre d'information et de documentation de Québec, l'enregistrement des visiteurs se fait directement sur place en même temps que la fiche client par le préposé qui accueille le visiteur.

7.3.2. Remise de la carte visiteur

Lors du départ d'un visiteur, un membre du personnel doit l'accompagner jusqu'à une zone externe et retourner la carte visiteur au poste d'accueil. L'heure de son départ est alors inscrite dans le registre des visiteurs.

7.4. Circulation en dehors des heures de bureau

7.4.1. Membre du personnel

Le membre du personnel dont les besoins reliés à sa fonction justifient un accès fréquent aux locaux de l'Institut en dehors des heures de bureau doit recevoir une approbation de son gestionnaire responsable afin d'ajuster ses droits d'accès.

Pour l'immeuble situé au 200, chemin Sainte-Foy à Québec, le membre du personnel reçoit une carte d'accès avec une pastille accolée afin de pouvoir y accéder entre 18 h et 7 h. Pour des besoins occasionnels, le membre du personnel peut obtenir une pastille temporaire avec l'autorisation de son gestionnaire responsable. Chaque pastille comporte un numéro unique qui correspond à une entrée au registre des pastilles temporaires.

Pour l'immeuble situé au 1200, avenue McGill College à Montréal, l'accès se fait avec sa carte d'accès. Pour des besoins occasionnels, les accès temporaires sont donnés directement sur la carte d'accès du membre du personnel avec l'autorisation de son gestionnaire responsable. Le préposé à l'accueil se charge d'obtenir ces accès temporaires.

7.4.2. Visiteur

Puisque le registre des visiteurs ne peut être tenu par le préposé à l'accueil en dehors des heures de bureau, tout visiteur doit être préalablement autorisé par le gestionnaire responsable du membre du personnel qui reçoit ledit visiteur.

De plus, ledit membre doit en informer le préposé à l'accueil. Le préposé à l'accueil préparera la carte visiteur et la remettra avec le registre des visiteurs audit membre.
Le membre du personnel qui reçoit ledit visiteur fera compléter le registre à ce dernier et lui remettra sa carte visiteur.

Au départ du visiteur, ledit membre doit l'accompagner jusqu'à une zone externe et inscrira l'heure de son départ dans le registre des visiteurs. Il est de la responsabilité dudit membre de

retourner la carte visiteur ainsi que le registre complété au préposé à l'accueil dès le jour ouvrable suivant.

7.4.3. Éclairage

Notez que les heures d'éclairage des locaux de l'Institut varient selon les zones et ne coïncident pas nécessairement avec les heures auxquelles les membres du personnel ont accès à ces zones. Selon les baux de l'Institut, les locaux de Québec et ceux de Montréal doivent être éclairés de 7 h 30 à 18 h 30.

7.4.4. Registre des pastilles temporaires

Le registre des pastilles temporaires contient les informations suivantes :

- le numéro de la carte d'identité temporaire;
- le numéro de la pastille temporaire;
- le nom et le prénom du membre du personnel qui emprunte la pastille;
- la signature dudit membre;
- la date d'emprunt de la pastille temporaire;
- une section commentaire.

7.5. Circulation des enfants

En règle générale, les enfants ne sont pas admis dans les locaux de l'Institut. Cependant, dans des cas exceptionnels, les enfants de moins de 14 ans peuvent être admis sans permis de circuler s'ils sont accompagnés d'un membre du personnel. Le membre du personnel concerné est responsable de la sécurité et du comportement des enfants pendant leur visite.

7.6. Nouveaux points d'entrée

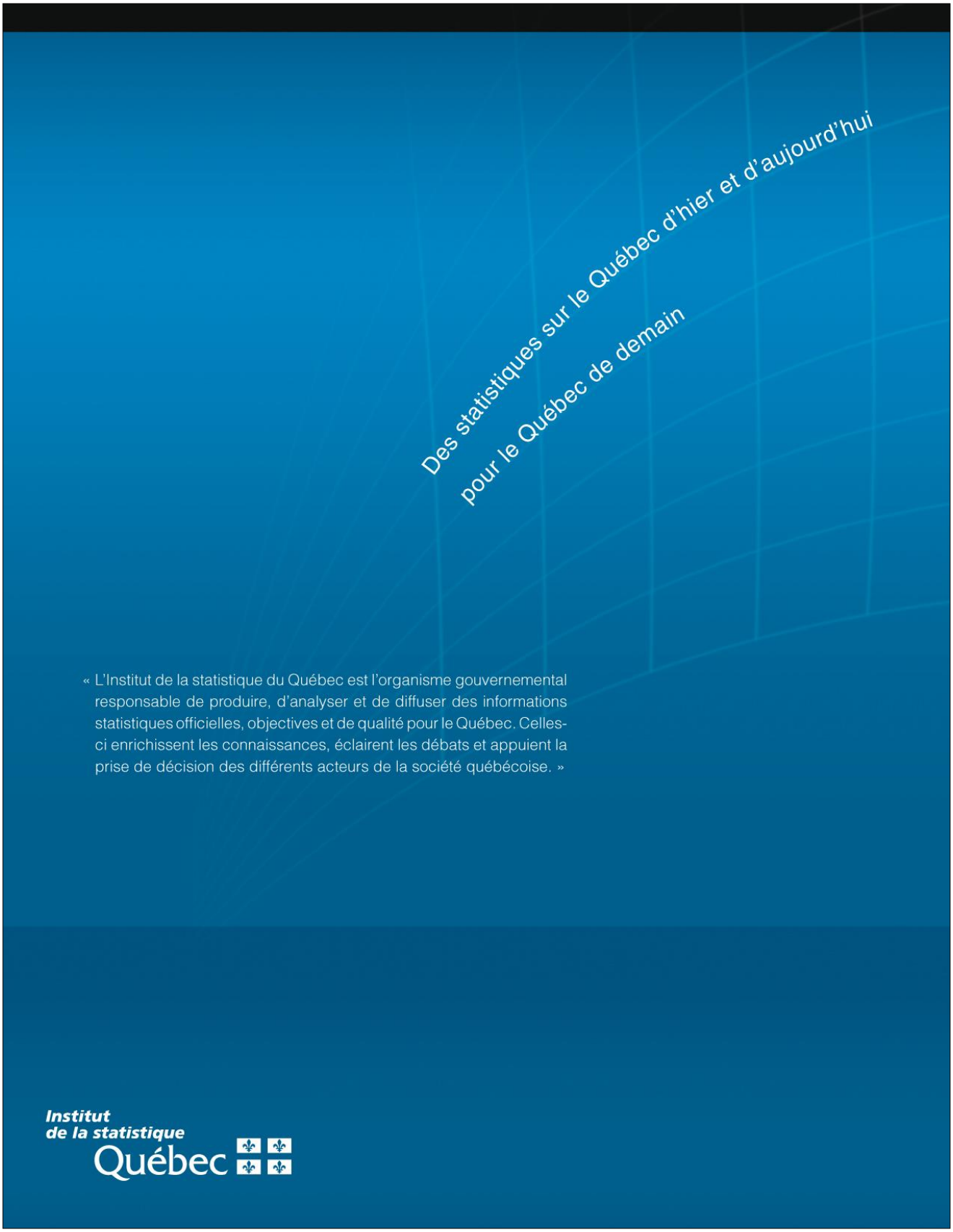
Toute modification des zones actuelles doit être communiquée au directeur général dès sa conception, et son approbation préalable est obligatoire.

7.7. Sanctions

Tout membre du personnel contrevenant aux dispositions de la présente politique est susceptible de se voir imposer des sanctions disciplinaires pouvant aller de l'avertissement au congédiement, selon la gravité de la faute commise. De plus, des sanctions pénales peuvent être administrées selon la faute.

26 février 2019
Date

Daniel Florea, directeur général


Des statistiques sur le Québec d'hier et d'aujourd'hui
pour le Québec de demain
« L'Institut de la statistique du Québec est l'organisme gouvernemental responsable de produire, d'analyser et de diffuser des informations statistiques officielles, objectives et de qualité pour le Québec. Celles-ci enrichissent les connaissances, éclairent les débats et appuient la prise de décision des différents acteurs de la société québécoise. »
Institut de la statistique Québec

Annexe 5

Cadre de gestion de la sécurité de l'information

INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Note

La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes.

Date d'approbation :	…
Responsable de la mise à jour :	Chef de la sécurité de l'information organisationnelle
Dernière mise à jour :	20 septembre 2023

Table des matières

1 Sommaire

Le cadre de gestion de la sécurité de l'information de l'Institut de la statistique du Québec (ISQ) vient appuyer la mise en œuvre des dispositions de la *Directive gouvernementale sur la sécurité de l'information*[1], en vigueur depuis le 8 décembre 2021. Cette directive s'applique aux organismes publics visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03). Elle a pour objet d'assurer adéquatement une prise en charge globale de la sécurité de l'information qu'un organisme public détient ou utilise dans l'exercice de ses 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.

Les travaux de révision du cadre gouvernemental de gestion de la sécurité de l'information se poursuivent. Pour que la directive de 2021 soit complète, des documents, lesquels remplacent ceux en vigueur, ont déjà été publiés, révisés, ou sont présentement en révision, notamment :

- 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, révisé sous l'Arrêté numéro 2022-04 du ministre de la Cybersécurité et du Numérique en date du 26 juillet 2022[2] ;
- le Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information, présentement en révision[3]. 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 (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).

Tous ces documents s'appuient sur la Politique gouvernementale de cybersécurité, adoptée en mars 2020, laquelle 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[4].

Sur le plan gouvernemental, les rôles et responsabilités nécessaires à une gouvernance forte et intégrée à cet égard sont assignés au dirigeant principal de l'information (DPI), qui occupe également le rôle de chef gouvernemental de la sécurité de l'information (CGSI) et de sous-ministre du ministère de la cybersécurité et du numérique (MCN). Le DPI et CGSI joue donc un rôle central en matière de gestion et de coordination de la sécurité de l'information gouvernementale.

1. 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].
2. 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].
3. 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. Adapté de : SECRÉTARIAT DU CONSEIL DU TRÉSOR (2009), *Directive sur la sécurité de l'information gouvernementale*, [En ligne]. [cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/DIR_securite_information_2021.pdf].

Pour ce qui est de chaque portefeuille, « les dirigeantes et dirigeants de l'information (DI) ont comme mandat d'appuyer le DPI dans son action, notamment par la mise en œuvre d'orientations, de politiques et de stratégies au sein des organismes publics auxquels ils sont rattachés concernant la gestion des technologies de l'information et la transformation numérique de leurs organisations. Ils sont les principaux conseillers en matière de ressources informationnelles auprès de leurs dirigeants, comme le prévoit entre autres la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement[5] ». Les DI assument également la fonction de chef délégué de la sécurité de l'information (CDSI).

Chaque portefeuille doit également constituer un centre organisationnel de cyberdéfense (COCD), qui relève du responsable organisationnel en cyberdéfense (ROCD).

Dans une organisation publique, ces rôles et responsabilités sont assignés au dirigeant d'organisme, au chef de la sécurité de l'information organisationnelle (CSIO), au conseiller organisationnel en sécurité de l'information (COSI), au coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) et son substitut, aux responsables des domaines connexes à la sécurité de l'information et aux comités sectoriels en sécurité de l'information.

- Ainsi, le dirigeant d'organisme public est le premier responsable de la sécurité de l'information relevant de son autorité. À ce titre, il doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques de sécurité de l'information.
- Le CSIO, quant à lui, joue le rôle de porte-parole du DPI/CGSI et du DI/CDSI auprès de son organisation, à laquelle il communique les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure également la coordination et la cohérence des actions en matière de sécurité de l'information qui sont posées par d'autres intervenants au sein de son organisation. De plus, il coordonne la contribution de son organisation aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.
- Le COSI apporte son soutien au CSIO sur le plan tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information.
- Le COMSI et son substitut collaborent étroitement avec le CSIO et le COSI en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités. Ils participent activement au réseau d'alerte gouvernemental et contribuent à la mise en place du processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) au sein de leur organisation, de la collaboration avec le responsable organisationnel en cyberdéfense (ROCD) du ministère des Finances, et du processus de gestion des risques à portée gouvernementale.

Aussi, le cadre de gestion de la sécurité de l'information précise les rôles des responsables des domaines connexes à la sécurité de l'information. Citons, à titre d'exemple, les rôles attribués aux détenteurs de l'information, au responsable de l'architecture de sécurité de l'information, au responsable de la sécurité physique et au responsable de la vérification interne. Ce cadre précise également le rôle des instances de coordination et de concertation appelées à soutenir le dirigeant d'organisme dans l'exercice de sa fonction de gouverne de la sécurité de l'information. Il s'agit de comités internes visant par exemple la gestion de la gouvernance, la gestion de crise et la continuité des services.

5. MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE (2023, mis à jour le 23 février), *Leadership de la transformation*, [En ligne]. [www.quebec.ca/gouvernement/politiques-orientations/vitrine-numeriqc/comprendre-et-suivre/leadership-de-la-transformation].

2 Introduction

Le présent cadre de gestion de la sécurité de l'information a pour objectif de compléter les dispositions de la Directive sur la sécurité de l'information gouvernementale. Il vient en complément de la politique de sécurité de l'information en décrivant, à cet égard, les rôles et les responsabilités nécessaires à une gestion intégrée de la sécurité de l'information au sein de l'ISQ.

3 Contexte

En plus du cadre légal et administratif gouvernemental, la Loi sur l'Institut de la statistique du Québec, ci-après nommée « Loi sur l'Institut », prévoit l'obligation de discrétion, c'est-à-dire que le statisticien en chef, 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 quelconque moyen, des renseignements obtenus en vertu de sa loi si ces révélations permettent de rattacher un renseignement à une personne, à une entreprise, à un organisme ou à une association en particulier.

Ainsi, les employés de l'ISQ ou toute autre personne dont les services sont utilisés par le statisticien en chef prêtent un serment de discrétion. Tous les employés ont une responsabilité à l'égard de la confidentialité et de la sécurité de l'information. Seul le personnel ayant besoin de consulter des données confidentielles dans l'exercice de ses fonctions est autorisé à y avoir accès. Des mesures de sécurité informatique, matérielle et administrative visent à protéger les données confidentielles contre tout accès non autorisé.

4 Définitions

Risque de sécurité de l'information à portée gouvernementale

Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale, qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

Incident de sécurité de l'information à portée gouvernementale

Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale qui nécessite une intervention concertée sur le plan gouvernemental.

Services communs de sécurité de l'information

Services, utilisés par plusieurs organismes publics, dont la gestion est centralisée.

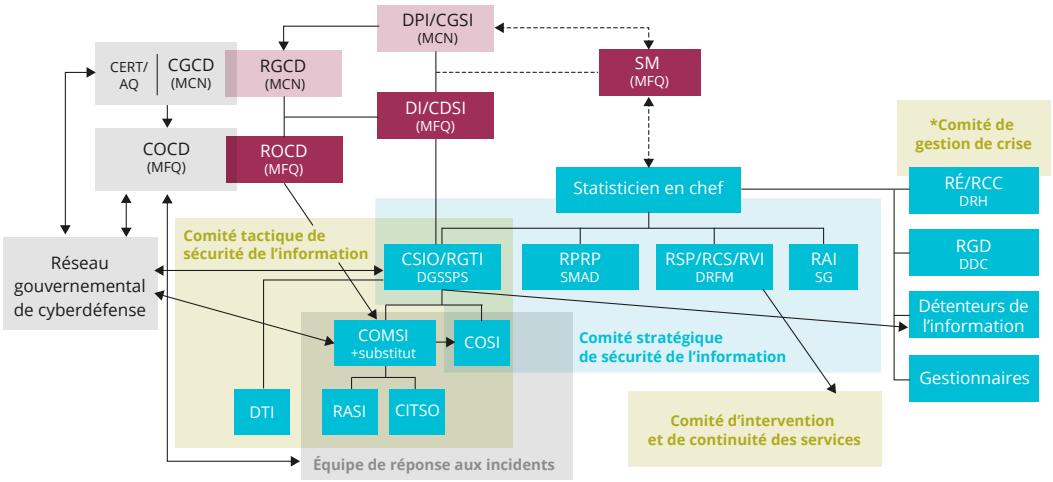
Domaines connexes

Domaines qui ne sont pas liés directement à la sécurité de l'information, mais pour lesquels des liens peuvent exister, par exemple : architecture de sécurité, sécurité physique, vérification interne, accès à l'information, protection des renseignements personnels, éthique.

Prendre note que d'autres définitions en lien avec ce document sont présentées dans le document « *Référence de la sécurité de l'information* ».

5 Organisation fonctionnelle de la sécurité de l'information

L'organisation fonctionnelle de la gestion de la sécurité de l'information qui est illustrée à la figure suivante présente les principales relations entre les intervenants et les instances de concertation (autorité fonctionnelle).



* Comité non inclus dans cette version du cadre de gestion en sécurité de l'information.

CGCD	Centre gouvernemental de cyberdéfense (MCN)
CITSO	Coordonnatrice de l'infrastructure technologique et de la sécurité opérationnelle
COCD	Centre organisationnel de cyberdéfense (MFQ)
COMSI	Coordonnateur organisationnel des mesures de sécurité de l'information et son substitut
COSI	Conseiller organisationnel en sécurité de l'information
CSIO	Chef de la sécurité de l'information organisationnelle
DI/CDSI	Dirigeant de l'information et chef délégué de la sécurité de l'information (MFQ)
DPI/CGSI	Dirigeant principal de l'information et chef gouvernemental de la sécurité de l'information (MCN)
RAI	Responsable de l'accès à l'information
RASI	Responsable de l'architecture de sécurité de l'information
RCC	Responsable du comité de crise
RCS	Responsable de la continuité des services
RÉ	Responsable de l'éthique
RGCD	Responsable gouvernemental de cyberdéfense (MCN)
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l'information
ROCD	Responsable organisationnel de cyberdéfense (MFQ)
RPRP	Responsable de la protection des renseignements personnels
RSP	Responsable de la sécurité physique
RVI	Responsable de la vérification interne

6 Rôles et responsabilités

La présente section décrit les instances de coordination et de concertation ainsi que les rôles et responsabilités en matière de sécurité de l'information au sein de l'ISQ, et ce, à tous les niveaux. Ces rôles et responsabilités peuvent être assumés par une seule et même personne et s'ajoutent alors aux fonctions actuelles.

6.1 Principaux intervenants

6.1.1 Statisticien en chef (dirigeant d'organisme)

Le statisticien en chef de l'ISQ est le premier responsable de la sécurité de l'information relevant de son autorité. Il doit :

- s'assurer de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable pour l'ISQ ;
- s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- désigner le chef de la sécurité de l'information organisationnelle (CSIO) au sein de l'ISQ. Le CSIO est un employé de niveau cadre qui a pour responsabilité de veiller à l'application des règles de gouvernance et de gestion établies en matière de sécurité de l'information sur le plan gouvernemental ;
- désigner les autres responsables de la sécurité de l'information au sein de l'ISQ. Le COMSI et son substitut sont des employés de niveau professionnel relevant de l'autorité administrative du CSIO. Le COSI est un employé de niveau professionnel relevant de la Secrétaire générale de l'ISQ ;
- désigner les détenteurs de l'information qui sont des employés de niveau cadre, qui ont pour responsabilité de s'assurer de la sécurité de l'information, et des ressources qui la sous-tendent, relevant de l'autorité de leur unité administrative ;
- assurer la concertation en matière de sécurité de l'information à l'intérieur de l'ISQ, notamment à travers son rôle de président du comité stratégique en sécurité de l'information ;
- approuver les orientations stratégiques de la sécurité de l'information de l'ISQ, les politiques, le cadre de gestion, les directives et les plans d'action en la matière et en assurer la mise en œuvre ;
- approuver les plans d'action ainsi que les bilans requis et les présenter aux instances gouvernementales concernées ;
- informer et mobiliser le personnel de l'ISQ quant aux décisions (orientations, politiques, directives, cadre de gestion, programme de formation, etc.) en ce qui concerne la confidentialité et la sécurité des informations détenues par l'ISQ.

6.1.2 Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO joue le rôle de porte-parole du DPI/CGSI ainsi que du DI/CDSI auprès de l'ISQ, auquel il communique les orientations et les priorités d'intervention gouvernementales et du portefeuille des finances en matière de sécurité de l'information. Il veille également à l'application des règles de gouvernance et de gestion établies sur le plan gouvernemental.

Il assiste le statisticien en chef pour ce qui est de la détermination des orientations stratégiques et des priorités d'intervention. De plus, il le représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. En outre, il est responsable :

- de soumettre au comité stratégique de la sécurité de l'information (CSSI) les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information ;
- de coordonner les actions et les mandats des responsables et des intervenants en sécurité de l'ISQ, notamment en présidant le comité tactique en sécurité de l'information (CTSI) ;
- d'assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein de l'ISQ par d'autres intervenants (détenteurs de l'information et unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique) ;
- de s'assurer de la contribution de l'ISQ au processus gouvernemental de gestion des risques et des incidents de sécurité de l'information ;
- de définir et de mettre en œuvre les processus officiels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ayant mis ou qui auraient pu mettre en péril la sécurité de l'information ;
- de s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information ;
- de coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information ;
- d'assurer le suivi de la mise en œuvre des recommandations du Conseil du trésor, du ministère de la Cybersécurité et du Numérique ou du dirigeant principal de l'information (DPI) ;
- de collaborer, conjointement avec le DPI et le CERT/AQ, à la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

Le CSIO est également responsable de la gestion des technologies de l'information (RGTI) (voir 6.2.1).

6.1.3 Conseiller organisationnel en sécurité de l'information (COSI)

Le COSI apporte son soutien au CSIO sur le plan tactique, notamment en ce qui concerne la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus officiels de sécurité de l'information.

Outre son rôle de soutien auprès du CSIO, le COSI est notamment chargé :

- de mettre en œuvre les orientations découlant des directives, des politiques et des pratiques ;
- de tenir à jour le registre d'autorité de la sécurité de l'information ;
- de produire les bilans et les plans d'action de sécurité de l'information ;
- de participer aux négociations des ententes de service et des contrats et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information ;
- d'assister les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information ;
- de soutenir le statisticien en chef et le CSIO dans l'organisation et la coordination des comités stratégiques et tactiques en sécurité de l'information.

De plus, le COSI joue un rôle clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information.

6.1.4 Coordonnateur organisationnel de mesures en sécurité de l'information (COMSI) et son substitut

Outre leur participation active au réseau d'alerte gouvernemental, lequel est mené par l'*Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise* CERT/AQ), maintenant une composante du centre gouvernemental de cyberdéfense (CGCD), le COMSI et son substitut ont notamment comme responsabilité :

- de contribuer à l'analyse des risques de sécurité de l'information, de déterminer les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées ;
- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information ;
- d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des infrastructures technologiques et des réseaux de télécommunication ;
- de collaborer étroitement avec le CSIO et de lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités.

6.1.5 Détenteurs de l'information

Les détenteurs d'information jouent un rôle clé en matière de sécurité de l'information, de processus d'affaires et de ressources relevant de la responsabilité de leurs unités administratives.

Ils assistent le statisticien en chef pour ce qui est de la gestion des risques de sécurité de l'information. À ce sujet, ils sont chargés :

- de participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans ;
- de catégoriser l'information relevant de leur responsabilité selon sa valeur en ce qui concerne la disponibilité, l'intégrité et la confidentialité et d'évaluer les préjudices liés à cette information ;
- de veiller à ce que les mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées ;
- de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus ;
- d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels.

6.2 Autres intervenants

6.2.1 Responsable de la gestion des technologies de l'information (RGTI)

Le RGTI doit, notamment :

- mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par l'ISQ, dont celles liées aux plans de reprise informatique en cas de sinistre et aux plans d'architecture ;
- mettre en place un cadre normatif de développement et d'acquisition assurant 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 de l'ISQ ;
- élaborer et mettre en œuvre les technologies et les fonctionnalités système tout en s'assurant de leur bon fonctionnement.

Le RGTI peut assumer lui-même ces responsabilités ou désigner des responsables tels qu'un architecte de sécurité de l'information (RASI), un responsable des infrastructures technologiques (RIT) et un responsable du développement et de l'acquisition des systèmes d'information (RDASI).

6.2.2 Responsable de la sécurité physique (RSP)

Le responsable de la sécurité physique met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Plus particulièrement, le responsable de la sécurité physique est chargé :

- de concevoir et de mettre en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités ;
- de s'assurer de la mise au rebut sécuritaire des supports de l'information ;
- d'élaborer et de mettre en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

6.2.3 Responsable de la continuité des services (RCS)

Le responsable de la continuité des services assure la gestion et la coordination du plan de continuité des services de l'ISQ. Plus particulièrement, il doit :

- coordonner l'élaboration du plan de continuité des services, veiller à sa mise en œuvre et en assurer la mise à jour ;
- assurer la planification et la coordination des tests initiaux et récurrents.

6.2.4 Responsable de la vérification interne (RVI)

Le RVI joue un rôle important dans la reddition de comptes en matière de sécurité de l'information, au chapitre de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il doit :

- évaluer, examiner ou vérifier l'application, la validité, l'adéquation et l'efficacité des règles, des mesures administratives et des moyens technologiques élaborés et mis en œuvre dans les processus d'affaires ;
- collaborer avec le CSIO à la définition et la mise en œuvre d'un plan d'audit en sécurité de l'information ;
- réaliser les enquêtes administratives liées aux incidents en sécurité de l'information qui lui sont soumis et informer le CSIO des résultats.

Le directeur de ressources financières et matérielles est RSP et également responsable de la continuité des services (RCS) et de la vérification interne (RVI).

6.2.5 Responsable de la protection des renseignements personnels (RPRP)

Le responsable de la protection des renseignements personnels 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 doit :

- communiquer au CSIO les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles ;
- 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.

6.2.6 Responsable de l'accès à l'information (RAI)

La responsable de l'accès à l'information répond aux demandes d'accès, soutient et conseille l'ISQ dans l'application des règles et des procédures prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ainsi qu'à celles imposées par la Loi sur l'Institut. Elle a pour objectif de maintenir l'équilibre entre l'esprit de la Loi et les nécessités de gestion de l'Institut, ainsi que de sensibiliser les autorités aux potentielles conséquences administratives majeures que pourrait avoir un dossier.

6.2.7 Responsable de l'éthique (RÉ)

La responsable de l'éthique veille à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information afin d'assurer la régularisation des conduites et la responsabilisation individuelle.

6.2.8 Responsable de la gestion documentaire (RGD)

La responsable de la gestion documentaire est chargée :

- de collaborer à la conception des systèmes informatiques, administratifs ou autres et de s'assurer, à toutes les étapes du cycle de vie de l'information, que ces systèmes ont les qualités nécessaires pour permettre une saine gestion des connaissances et du patrimoine informationnel, de la préservation des preuves et du respect des lois ;
- de collaborer étroitement avec les détenteurs de l'information ainsi qu'avec le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

6.2.9 Gestionnaires

Les gestionnaires sont responsables de la mise en œuvre, auprès du personnel relevant de leur autorité, des dispositions de la politique et des principes directeurs encadrant la SI. Ils doivent principalement :

- informer leur personnel de leurs obligations, des directives, des normes et des procédures en vigueur ainsi que des modalités liées à leur mise en œuvre, et sensibiliser à la nécessité de s'y conformer ;
- s'assurer que les ressources informationnelles sont utilisées en conformité avec les principes généraux et les exigences de la politique de SI ;
- accorder les accès aux systèmes et aux informations à leur personnel et veiller à ce qu'il accède uniquement à l'information nécessaire à l'exercice de ses fonctions.

6.3 Intervenants gouvernementaux et du portefeuille Finances

Les intervenants suivants et leurs rôles sont détaillés dans la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (Loi) et la Directive gouvernementale de sécurité de l'information de 2021 (Directive) :

Dirigeant principal de l'information (DPI) et chef gouvernemental de la sécurité de l'information (CGSI)

« Le sous-ministre du ministère de la Cybersécurité et du Numérique agit à titre de dirigeant principal de l'information. » (Article 6 de la Loi)

« Le dirigeant principal de l'information agit, pour l'Administration publique, à titre de chef gouvernemental de la sécurité de l'information, en assumant les responsabilités prévues à l'article 12.6 » (Article 7.1, alinéa 1 de la Loi)

« Le chef gouvernemental de la sécurité de l'information assume les responsabilités découlant de la Loi et de ses textes d'application. » (Article 5 de la Directive)

Responsable gouvernemental de la cyberdéfense (RGCD)

« Le CGSI (…) désigne, parmi les membres du personnel d'encadrement sous sa direction, un responsable gouvernemental de cyberdéfense dont le rôle est de voir au bon fonctionnement du Centre gouvernemental de cyberdéfense » (Article 5, alinéa 4 de la Directive)

Centre gouvernemental de la cyberdéfense (CGCD)

« Centre gouvernemental de cyberdéfense : l'unité administrative spécialisée en sécurité de l'information visée à l'article 12.5 de la Loi » (Article 2, alinéa 1 de la Directive)

Dirigeant de l'information (DI) et chef délégué de la sécurité de l'information (CDSI)

Tout ministre titulaire d'un ministère désigne, parmi les membres du personnel de direction qui relèvent directement de son sous-ministre et après recommandation du dirigeant principal de l'information, un dirigeant de l'information pour son ministère ainsi que pour l'ensemble des autres organismes publics relevant de son portefeuille. (Article 8 de la Loi)

Le chef délégué de la sécurité de l'information assume, sous le lien fonctionnel du CGSI et pour les organismes publics auxquels il se rattache, les responsabilités découlant de la Loi et de ses textes d'application. (Article 6 de la Directive)

Responsable organisationnel de la cyberdéfense (ROCD)

« Le CDSI (…) désigne, parmi les membres du personnel d'encadrement sous sa direction et conformément aux indications d'application du chef gouvernemental de la sécurité de l'information, un responsable opérationnel de cyberdéfense dont le rôle est de voir au bon fonctionnement du Centre opérationnel de cyberdéfense » (Article 6, alinéa 2 de la Directive)

Centre organisationnel de la cyberdéfense (COCD)

« Un ministre doit maintenir, pour son ministère et l'ensemble des organismes relevant de son portefeuille, une unité administrative spécialisée en sécurité de l'information appelée Centre opérationnel de cyberdéfense. » (Article 9 de la Directive)

6.4 Instances de concertation

Les comités sont des instances organisationnelles de concertation et d'intervention dans la mise en œuvre de la sécurité de l'information et de la continuité des services.

6.4.1 Comité stratégique de la sécurité de l'information (CSSI)

Le comité stratégique de la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information. Plus particulièrement, il veille à :

- examiner et à entériner les recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'ISQ, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information ;
- analyser et à entériner les recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information.

En cas d'incident critique de sécurité de l'information, le comité stratégique est appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, il a pour rôle :

- d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information ;
- d'adopter la déclaration de sinistre proposée par le chef de la sécurité de l'information organisationnelle et d'approuver les budgets spéciaux correspondants ;
- de décider du déploiement ou non des plans de continuité des services ;
- d'adopter les recommandations concernant le délestage, en totalité ou en partie, des activités ;
- d'approuver les stratégies de communication avec les médias.

Ce comité est présidé par le statisticien en chef ou son représentant. Il comprend, notamment, le chef de la sécurité de l'information organisationnelle, la responsable de la protection des renseignements personnels, la responsable de l'accès à l'information et le responsable du plan de continuité des services. Le COSI est le secrétaire du comité. Les autres intervenants sont invités au besoin.

Aussi, ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision.

6.4.2 Comité tactique de la sécurité de l'information (CTSI)

Le comité tactique de la sécurité de l'information reçoit et traite les demandes en matière de SI. Plus particulièrement, il a comme mandat :

- d'analyser toute question relative aux projets d'acquisition, de développement et de refonte de systèmes dans les lignes d'affaires ayant une incidence sur les ressources informationnelles ou sur la prestation électronique de service qui recueille, utilise, conserve, communique ou détruit des informations ;
- de diriger la mise en œuvre et l'évolution du plan d'action triennal en sécurité de l'information (PTSI).

Le comité est présidé par le CSIO. Il est composé du responsable de l'architecture de sécurité de l'information, du responsable du développement ou de l'acquisition de systèmes d'information et du coordonnateur organisationnel de gestion des incidents. Le COSI est le secrétaire du comité.

Il peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans son mandat et ses prises de décision, par exemple les détenteurs de l'information et le responsable de la continuité des services.

6.4.3 Comité d'intervention et de continuité des services (CICS)

En cas d'incident critique de la SI, le comité est appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, il a principalement pour rôle de :

- mettre en œuvre des stratégies permettant d'assurer la prise en charge des incidents critiques de la SI ;
- proposer des orientations à suivre ou des mesures à prendre en cas de sinistre ;
- formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'ISQ ;
- préparer les communications avec les médias.

Le comité a aussi comme mandat d'assurer la continuité des services. Il a pour rôle, notamment :

- de procéder à l'évaluation des dommages ;
- de recommander au comité de crise l'adoption d'une déclaration de sinistre ;
- d'assurer la mise en œuvre du plan de mobilisation ;
- d'assurer la coordination avec les intervenants extérieurs.

Ce comité est présidé par le directeur des ressources financières et matérielles qui assume les rôles de RCS, de RSP et de RVI. Il est composé également de la directrice des ressources humaines, du directeur des technologies de l'information, de la directrice de la diffusion et des communications (DDC), pour le volet communication avec les médias, ainsi que du CSIO et du COSI, qui est le secrétaire du comité. Les autres intervenants sont invités au besoin.

7 Disposition finale

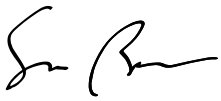
7.1 Date d'entrée en vigueur

Le cadre de gestion de la sécurité de l'information entre en vigueur à la date d'approbation par le statisticien en chef et demeure en application tant et aussi longtemps qu'il n'est pas abrogé, modifié ou remplacé par un autre cadre de gestion ou une directive.

8 Approbation

2023-10-03

Date



Simon Bergeron, statisticien en chef

Annexe 6

Procédure de traitement des demandes d'accès aux données de recherche

INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Note

La forme masculine est utilisée dans le présent document afin d'alléger le texte.

Date d'approbation :	22 août 2022
Unité responsable :	Direction de la protection et de l'optimisation des données administratives

Table des matières

Processus d'accès aux données de recherche – Évolution d'une demande d'accès

	Soumission d'une demande d'accès	Évaluation de la demande	Engagements contractuel et administratif	Préparation du fichier de recherche	Accès au fichier de recherche, exploitation des données et diffusion de résultats	Suivi du projet	Fermeture du projet
Équipe de recherche	▸ Explorer les banques de données ainsi que les variables disponibles et consulter la trousse de démarrage ▸ Effectuer une simulation de coûts, si souhaité ▸ Préparer la demande (formulaire, pièces justificatives et liste de vérification des documents) ▸ S'assurer que tous les documents soumis sont présents et à jour ▸ Soumettre la demande dans la Zone recherche	▸ Fournir les documents et les informations demandés par l'ISQ aux fins de l'évaluation de la demande ▸ Le cas échéant, obtenir les autorisations nécessaires à l'ajout, au fichier de recherche, de données externes	▸ Prendre connaissance des règles de sécurité et de protection des renseignements personnels contenues dans le contrat ▸ Signer le contrat et l'engagement à la confidentialité (équipe de recherche et organisme de rattachement)		▸ Participer à la séance d'orientation tenue par l'ISQ (équipe de recherche) ▸ Se prêter à l'assermentation ▸ Consulter le fichier de recherche dans un environnement sécurisé (dans un CADRISQ ou à distance) ▸ Exploiter les données ▸ Diffuser uniquement des résultats statistiques respectant les règles de confidentialité de l'ISQ	▸ S'assurer que le renouvellement de l'approbation éthique du projet est fourni tout au long de la période d'accès autorisée ▸ À la fin de la période d'accès autorisée, demander une prolongation si la recherche n'est pas terminée ▸ Informer l'ISQ des productions scientifiques découlant de l'exploitation du fichier de recherche	▸ Informer l'ISQ de la fin du projet de recherche nécessitant l'exploitation du fichier de recherche et l'autoriser à entamer la fermeture du projet ▸ Remettre à l'ISQ l'ensemble des éléments d'authentification fournis aux personnes autorisées
Institut de la statistique du Québec (ISQ)	▸ Accompagner le chercheur dans la définition de ses besoins	▸ Évaluer la faisabilité technique de la demande et la disponibilité des données ▸ Estimer, si nécessaire, la taille de la cohorte ▸ Fournir une évaluation sommaire des coûts au chercheur ▸ Évaluer la protection des renseignements personnels ▸ Informer le chercheur des modalités d'accès aux données	▸ Préparer et transmettre le contrat et l'engagement à la confidentialité ▸ Signer le contrat	▸ Procéder à la sélection des individus visés pour la recherche parmi les banques de données sous sa responsabilité ▸ Procéder à l'appariement des banques de données, si nécessaire (méthode probabiliste) ▸ Sélectionner et extraire les variables autorisées ▸ Créer le fichier de recherche pour le projet	▸ Tenir une séance d'orientation obligatoire destinée à l'équipe de recherche (sécurité, protection des renseignements personnels et règles de contrôle du risque de divulgation) ▸ Assermentation de l'équipe de recherche ▸ Fournir aux chercheurs un environnement sécurisé pour accéder aux données, dans lequel des logiciels statistiques sont mis à leur disposition (ex. : STATA, R, SAS, SPSS) ▸ Rendre accessibles le fichier de recherche et les résultats statistiques des travaux du chercheur, selon les modalités convenues ▸ Vérifier les résultats statistiques avant leur diffusion pour s'assurer qu'ils respectent les règles de confidentialité de l'ISQ	▸ Inscrire au dossier du projet les renouvellements d'approbation éthique obtenus par le chercheur ▸ Publier les références des productions scientifiques découlant de l'exploitation des données sur le site Web des services d'accès aux données	▸ Désactiver les accès du chercheur et de son équipe ▸ Détruire les données selon les modalités convenues ▸ Conserver les programmes et la documentation propres au projet à la demande du chercheur

Préambule

Ce document présente les étapes du traitement des demandes d'accès aux données pour des fins de recherche à l'Institut de la statistique du Québec (ISQ) ainsi que les principaux rôles et responsabilités du chercheur et de l'ISQ.

Soumission d'une demande d'accès

La soumission d'une demande d'accès débute lorsque le chercheur, muni de son protocole de recherche (ou d'une description détaillée de ses activités de recherche) et de l'approbation d'un comité d'éthique de la recherche (le cas échéant), se rend sur le site Internet des services d'accès aux données de l'ISQ pour préparer sa demande. Pour le faire correctement, le chercheur peut consulter la documentation sur le site, dont la trousse de démarrage du chercheur et la liste des banques de données disponibles. Il peut également effectuer une simulation de coûts pour son projet.

Une fois la création d'un compte sur le site Web des services d'accès aux données de recherche autorisée par l'ISQ, le chercheur admissible peut remplir le formulaire de demande en ligne et y annexer tous les documents requis. Il doit s'assurer que ces documents sont à jour et que l'information que l'on y retrouve est cohérente d'un document à l'autre.

Enfin, lorsque sa demande est complète, le chercheur peut soumettre sa demande et suivre l'évolution de son traitement sur le site.

Tout au long de cette étape, le personnel de l'ISQ est disponible pour aiguiller le chercheur.

Évaluation de la demande

Après la soumission de la demande, le personnel de l'ISQ vérifie la disponibilité des données demandées et évalue la faisabilité technique de la demande. Il fournit également une évaluation sommaire des coûts. Une fois cette évaluation acceptée par le chercheur, une évaluation de la protection des renseignements personnels est effectuée et un rapport d'évaluation est rédigé. Enfin, le personnel de l'ISQ informe le chercheur des modalités d'accès aux données recommandées pour son projet de recherche.

En parallèle, le chercheur est amené à fournir l'information requise par le personnel de l'ISQ aux fins de l'évaluation de la demande et à transmettre les documents les plus à jour.

Le délai de traitement de la demande à cette étape dépend, en grande partie, de la capacité du chercheur à répondre rapidement aux demandes de précision de l'ISQ et à s'assurer que les informations inscrites dans le formulaire de demande correspondent à celles qui se trouvent dans les documents officiels (principalement le protocole de recherche ou la description détaillée des activités de recherche) approuvés par le comité d'éthique de la recherche. Le chercheur doit également s'assurer de transmettre à l'ISQ les renouvellements de l'approbation éthique dès qu'il les reçoit. Les délais nécessaires à l'obtention des données sont tributaires de plusieurs facteurs, dont la complexité des appariements, la multiplicité des sources de données ainsi que le recours à des données d'enquêtes ou à des renseignements non désignés.

Engagements contractuel et administratif

L'accès aux données est conditionnel à la signature, par le chercheur et son organisme de rattachement, d'un contrat avec l'ISQ. C'est ce contrat qui constitue l'autorisation officielle de l'accès aux données requises pour la recherche. Ce contrat précise quels sont les données autorisées pour la recherche, les rôles et responsabilités de chaque partie, les modalités d'accès aux données, les règles de confidentialité et de sécurité ainsi que les frais de production du fichier de recherche.

Un contrat modèle est disponible dans la trousse de démarrage afin que le chercheur puisse prendre connaissance du contenu de celui-ci. La prise de connaissance précoce de ce document permet d'accélérer la signature du contrat qui sera ultimement conclu. Il est donc de la responsabilité du chercheur d'amorcer la discussion avec son organisme de rattachement dès le début de sa démarche afin d'accélérer la signature du contrat.

Le chercheur et son équipe doivent prendre connaissance des règles de sécurité et de protection des renseignements personnels de l'ISQ contenus dans le contrat avant d'avoir accès aux données.

Enfin, chaque membre de l'équipe de recherche désirant avoir accès aux données doit signer un engagement à la confidentialité.

Préparation du fichier de recherche

Une fois l'évaluation finale des coûts acceptée par le chercheur et l'autorisation obtenue pour le projet, comme en fait foi la signature des engagements contractuel et administratif par les parties, le personnel de l'ISQ procède à la sélection des individus visés pour la recherche. Si nécessaire, il procède à l'appariement des banques de données. Ensuite, il sélectionne et extrait les variables autorisées et crée le fichier de recherche, qui est déposé dans une zone d'accès privée prévue pour le chercheur et les membres autorisés de son équipe.

Lorsque des données externes sont requises pour la recherche, le chercheur doit fournir l'autorisation du détenteur de ces données ainsi que les fichiers de données visés. Cette autorisation peut prendre la forme d'une autorisation d'un ministère ou d'un organisme (en vertu de l'article 67.2.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1] ou d'articles de loi équivalents utilisés antérieurement), d'une autorisation du directeur des services professionnels ou du directeur général d'un établissement de santé – pour des données provenant du dossier électronique du patient (en vertu de l'article 19.2 de la *Loi sur les services de santé et les services sociaux*[2]) – ou d'un formulaire de consentement signé par les participants recrutés pour la recherche.

Accès au fichier de recherche, exploitation des données et diffusion de résultats

Afin d'avoir accès au fichier de recherche, le chercheur et les membres autorisés de son équipe doivent participer à une séance d'orientation obligatoire tenue par l'ISQ lors de laquelle les règles de sécurité et de protection des renseignements personnels ainsi que les règles de contrôle du risque de divulgation propres au projet de recherche leur seront expliquées. Ils doivent également être assermentés par l'ISQ. L'équipe de recherche peut alors consulter et exploiter les données, soit sur place, dans l'un des centres d'accès aux données de recherche de l'ISQ (CADRISQ)

1. RLRQ, chapitre A-2.1.
2. RLRQ, chapitre S-4.2.

mis à la disposition des chercheurs, soit via un accès à distance à l'environnement sécurisé de l'ISQ. Dans ce dernier cas, l'accès est donné à un fichier de microdonnées accessible à distance (FMAD), lequel a subi certaines modifications (masquage) par rapport au fichier de recherche disponible au CADRISQ afin que les risques de divulgation de renseignements confidentiels soient réduits.

Par ailleurs, dans les cas où le chercheur a obtenu, au préalable, le consentement exprès des participants pour accéder aux données administratives demandées (et que ce consentement précise un lieu de conservation des données extérieur à l'environnement de l'ISQ), nous honorons ce consentement en autorisant le chercheur à avoir accès aux données sans qu'elles fassent préalablement l'objet de traitements de masquage.

L'ISQ, de son côté, fournit au chercheur un environnement sécurisé pour accéder aux données, dans lequel des logiciels statistiques, comme STATA, R, SAS et SPSS, sont mis à sa disposition.

Avant de diffuser des résultats, le chercheur doit s'assurer de respecter les règles de confidentialité de l'ISQ. À cet égard, le personnel de l'ISQ fournit un guide au chercheur qui détaille, notamment, les règles de vérification des résultats pour minimiser le risque de divulgation de renseignements personnels et effectue une vérification des résultats statistiques avant leur diffusion pour s'assurer qu'ils respectent les règles de confidentialité. L'ISQ peut, à la demande du chercheur, rendre accessibles des résultats intermédiaires à distance (c'est-à-dire des résultats pour lesquels les règles de confidentialité n'ont pas été appliquées) afin que le chercheur et son équipe puissent en discuter avant de finaliser leurs analyses.

Suivi du projet

Tout au long de la période d'accès aux données autorisée, le chercheur doit s'assurer que le renouvellement de l'approbation éthique du projet est fourni à l'ISQ, qui le consigne ensuite dans le dossier de la recherche. Le chercheur doit également informer l'ISQ des productions scientifiques découlant de l'exploitation du fichier de recherche. L'ISQ doit, comme le prévoit sa loi constitutive, publier les références de ces productions scientifiques dans un registre sur le site Web des services d'accès aux données.

À la fin de la période d'accès autorisée, le chercheur doit effectuer une demande de prolongation si la recherche n'est pas terminée.

Fermeture du projet

À la fin du projet de recherche nécessitant l'exploitation du fichier de recherche, le chercheur doit informer l'ISQ de ce fait et l'autoriser à entamer la fermeture du projet. Il doit également remettre à l'ISQ l'ensemble des éléments d'authentification fournis aux personnes autorisées de son équipe.

Le personnel de l'ISQ procède alors à la désactivation des accès du chercheur et des membres de son équipe ainsi qu'à la destruction des données selon le calendrier de conservation de l'ISQ. À la demande du chercheur, l'ISQ peut conserver certaines informations, comme les programmes informatiques, les résultats statistiques non diffusés et la documentation propres au projet.

« La statistique au
service de la société :
la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec

Annexe 7

Processus de gestion et de traitement des incidents en sécurité de l'information

INSTITUT
DE LA
STATISTIQUE
DU QUÉBEC

Québec

Historique des modifications

Version	Date	Créé / modifié par	Description de la modification
0.8	2006-11-28	Équipe de rédaction : • Benoît Jourdain (Horus IT) • André Castonguay (ISQ)	Version initiale du dossier
0.9	2019-02-06	Madeleine Filion	Version modifiée pour tenir compte des nouveautés et ajustements de la nouvelle directive gouvernementale en sécurité de l'information
0.91	2019-01-01	Équipe sécurité	Validation et ajustements
0.92	2019-03-05	Équipe sécurité	Validation et ajustements
0.93	2019-03-08	Équipe sécurité	Validation et ajustements
0.94	2019-03-11	Équipe sécurité	Validation et ajustements
0.95	2019-03-12	Samuel Bonneau	Intégration des commentaires
0,98	2019-09-19	Dany Matte	Ajustements linguistiques
0,99	2021-07-09	Présentation comité de direction Stéphane Lefebvre, ROSI	Ajustements mineures dus aux changements à l'organigramme
1.0	2021-09-07	Approbation du ROSI	Dépôt pour publication à l'Intranet

Note

La forme masculine utilisée dans ce document désigne tout aussi bien les femmes que les hommes. Les appellations DGAs et DG désignent respectivement les directeurs généraux et le Statisticien en chef.

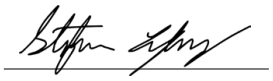
Unité responsable de la mise à jour :	Direction des technologies de l'information
Date de la signature :	7 septembre 2021
Signature :	 Stéphane Lefebvre, ROSI

Table des matières

Contexte

Le gouvernement du Québec a déposé en mai 2018 la Stratégie pour une administration publique numérique[1]. Cette stratégie mise sur la rapidité, la simplicité, l'ouverture, l'agilité et l'innovation pour déployer une administration publique centrée sur la personne. L'un des enjeux le plus fondamental pour livrer ses services est la sécurité de l'information.

La préoccupation de la sécurité doit ainsi se retrouver dans les différents aspects de la gouvernance de l'Institut de la statistique du Québec (ISQ) et notamment dans la définition des responsabilités, les processus de gestion et les mécanismes de contrôle et de suivi.

Le rythme d'apparition de nouvelles vulnérabilités (hameçonnage, rançongiciels, etc.) et le risque grandissant d'atteinte à la vie privée avec l'adoption massive des médias sociaux, des progiciels et des services infonuagiques sont en constante augmentation. Il s'avère donc pratiquement impensable de maintenir ou d'améliorer les mesures de prévention et de réaction aux incidents de sécurité sans se doter de moyens humains, matériels et logiciels suffisants en adéquation avec les risques appréhendés.

L'implantation d'un processus de gestion et de traitement des incidents en sécurité de l'information axé principalement sur la prévention, la détection et la réponse aux incidents est essentielle à l'ISQ.

Le *Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information* présente une approche de détermination et de suivi du traitement des risques et des incidents susceptibles d'avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect des droits fondamentaux à la protection des renseignements personnels et au respect de la vie privée, sur l'image du gouvernement ou sur la prestation de services d'autres organismes publics. À cet effet, l'ISQ doit ajuster ses façons de faire de manière à prendre appui sur de nouveaux modèles de documents gouvernementaux, ce qui justifie la révision du présent document.

Conformément au *Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information* en ce qui a trait à la gestion des incidents en sécurité de l'information, autant les administrations que les grandes entreprises s'appuient sur la méthodologie Computer Emergency Response Team (CERT) de l'Université Carnegie-Mellon à Pittsburgh qui en a jeté les bases en 1988. Les tâches prioritaires assumées par l'unité permanente qui constitue le CERT sont les suivantes :

- Centralisation des demandes d'assistance à la suite d'incidents de sécurité (attaques) sur les réseaux et les systèmes d'information : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- Traitement des alertes et réaction aux attaques informatiques : analyses techniques, échanges d'information avec d'autres CERT, contribution à des études techniques spécifiques ;
- Établissement et maintien d'une base de données des vulnérabilités ;
- Prévention par la diffusion d'information sur les précautions à prendre pour minimiser les risques d'incidents ou, au pire, leurs conséquences ;

Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseau, opérateurs et fournisseurs d'accès Internet, CERT nationaux et internationaux.

1. tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/strategie_apn/strategie_APN.pdf

1 But

Le but du processus est de permettre à l'ISQ d'atténuer les risques et de s'assurer qu'en cas d'incident en sécurité de l'information, les actions appropriées seront posées, les personnes concernées seront contactées et, le cas échéant, les actions nécessaires à la tenue d'une enquête seront réalisées correctement.

Le présent document vise donc à définir le **processus de gestion et de traitement des incidents en sécurité de l'information**, les structures à mettre en place pour le supporter ainsi que les rôles et responsabilités des divers intervenants impliqués.

On y distingue deux types d'incidents :

1. Incident à portée gouvernementale

   Les risques à portée gouvernementale[1] sont avant tout des risques dont les conséquences vont au-delà des limites d'un seul organisme public. Dans ce cas, l'organisme public concerné n'est plus seul à devoir se prononcer sur l'application d'un traitement ou d'une mesure correctrice, car il n'est pas le seul à subir les conséquences de l'incident. C'est le cas des incidents aux conséquences potentiellement graves pour la population ou pour l'image du gouvernement, ainsi que celles qui sont susceptibles de perturber les services offerts par d'autres organismes publics.

   Parallèlement, certaines conséquences ne peuvent être prises en charge que par l'organisme public qui y est exposé de façon directe. C'est notamment le cas pour tous les incidents liés aux interdépendances en matière d'information ou de traitement de l'information entre organisations qui, généralement, ont des répercussions à plus d'un endroit. Ces types d'incidents devraient également être considérés comme étant à portée gouvernementale.

2. Incident à portée sectorielle

   Les incidents à portée sectorielle sont ceux dont la portée se limite à un seul organisme public. On les classe ainsi en vue de permettre l'élaboration de processus de gestion ciblés.

1. Cadre de gestion des risques et des incidents à portée gouvernementale section 3.3.1 [tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_risques_incidents.pdf]

2 Objectif

Le processus de gestion et de traitement des incidents en sécurité de l'information vise à minimiser les dommages provenant d'incidents de sécurité et de défauts de fonctionnement, à les surveiller et à en tirer des leçons. Pour ce faire :

- les incidents affectant la sécurité de l'information doivent être signalés le plus rapidement possible par l'intermédiaire des filières de gestion appropriées ;
- tous les employés et tous les fournisseurs et prestataires de services doivent être informés des procédures utilisées pour le signalement des différents types d'incidents (infraction à la sécurité, menace, faiblesse ou mauvais fonctionnement) qui pourraient avoir des répercussions sur la sécurité des actifs informationnels ou sur les partenaires ayant une entente avec l'ISQ.
- l'ISQ doit exiger de ses partenaires qu'ils signalent tout incident observé ou soupçonné le plus rapidement possible au point de contact désigné ;
- l'ISQ doit établir un processus administratif officiel de manière à pouvoir réagir correctement à ces incidents. Il pourra s'avérer nécessaire de recueillir des éléments de preuve dès que possible à la suite des incidents et, selon la gravité établie dans le bilan, porter plainte aux autorités compétentes ou demander la tenue d'une enquête.

3 Portée

Ce processus s'applique à tout incident de sécurité de l'information, qu'il soit réel ou suspecté, ou qu'il s'agisse d'une tentative susceptible d'affecter la disponibilité, l'intégrité et la confidentialité d'actifs informationnels, de données, d'applications, d'équipements, d'applications bureautiques et d'infrastructures technologiques (logiciels et matériels, téléphonie, télécommunications, etc.) détenus par l'ISQ.

Le processus s'adresse à :

- Tout le personnel de l'ISQ, y compris les sous-traitants et les partenaires ;
- Toute personne témoin d'un incident de sécurité dans le cadre d'une prestation de travail, d'une entente de services effectués pour le compte d'un partenaire ou d'un fournisseur ou de toute autre situation circonstancielle.

4 Hors portée

Le processus de gestion et de traitement des incidents en sécurité de l'information défini dans le présent document couvre toute l'infrastructure technologique de l'ISQ incluant les équipements bureautiques et les appareils mobiles (portables, tablettes, clés USB et support externes, etc.).

Toutefois, il exclut les incidents associés :

- à la continuité des services (incendie, inondation, séisme, etc.). Ces incidents sont traités dans le plan de continuité des services essentiels de l'ISQ ;
- aux services impartis ou fournis par un organisme externe (ex. RISQ, RIQ, SAGIR, etc.) ;
- aux incidents technologiques n'ayant pas d'incidence sur la sécurité de l'information ;
- au traitement sans conséquence des virus et des logiciels malveillants.

5 Intervenants

Structure de gouvernance en sécurité de l'information à l'ISQ

Le cadre de gestion en sécurité de l'information de l'ISQ, en vigueur depuis le 16 mai 2017, vient appuyer la mise en œuvre des dispositions de la Directive sur la sécurité de l'information gouvernementale. Il est un complément de la politique de sécurité de l'information, aussi en vigueur depuis le 16 mai 2017. Il décrit :

- les rôles et les responsabilités nécessaires à une gestion intégrée de la sécurité de l'information au sein de l'ISQ ;
- le rôle des instances de coordination et de concertation appelées à soutenir le dirigeant d'organisme dans l'exercice de sa fonction de gouverne de la sécurité de l'information.

Plus précisément, pour la gestion des incidents en sécurité de l'information :

Équipe de réponse aux incidents en sécurité de l'information

Équipe interne à l'ISQ, dont le rôle est de gérer et de traiter les incidents affectant l'intégrité, la disponibilité ou la confidentialité de l'information. Cette équipe peut être soutenue dans ses activités par une expertise reconnue, externe à l'organisation, comme le CERT/AQ.

Cette équipe, dirigée par le responsable organisationnel de la sécurité de l'information (ROSI), est constituée du coordonnateur organisationnel de la gestion des incidents (COGI), du conseiller organisationnel en sécurité de l'information (COSI), du responsable de la gestion des technologies de l'information (RGTI) et de ressources spécialisées en technologies de l'information.

Responsable organisationnel de la sécurité de l'information

Dans le cadre du processus de gestion et de traitement des incidents, le ROSI, assisté par le COSI, a les responsabilités suivantes :

- Assurer la coordination de l'équipe de réponse ;
- Élaborer et mettre en œuvre le processus d'escalade au palier hiérarchique supérieur et au responsable de la protection des renseignements personnels ;
- Assurer la communication auprès des intervenants internes et externes ;
- Convoquer le comité de crise au besoin ;
- Approuver les communiqués internes à propos des incidents ;
- Assurer la liaison avec les partenaires d'affaires de l'ISQ lorsqu'ils sont concernés.

Conseiller organisationnel en sécurité de l'information

- Assister le ROSI dans la réalisation des activités à réaliser en sécurité de l'information.

Responsable de la gestion des technologies de l'information

- Assurer la disponibilité des ressources humaines en technologies de l'information en cas d'incident ;
- Désigner des responsables informatiques pour le traitement et la résolution de l'incident en fonction de la nature et de la gravité de celui-ci ;
- Autoriser le recours à des services externes.

Coordonnateur organisationnel de la gestion des incidents et son substitut

- Assurer la mise en place et le suivi du processus de gestion et de traitement des incidents et en assurer la diffusion auprès des utilisateurs ;
- Assurer la mise en place et le suivi des procédures opérationnelles de gestion et de traitement des incidents, et en assurer la diffusion auprès des utilisateurs ;
- S'assurer de la détection et de la gestion des risques d'atteinte à la sécurité de l'information ;
- Faire rapport au ROSI et lui rendre compte de l'état d'avancement du processus de gestion et de traitement des incidents ;
- Apporter le soutien nécessaire au ROSI pour l'élaboration du processus d'escalade ;
- Assurer la communication avec le COSI, le CERT/AQ, les coordonnateurs organisationnels de la gestion des incidents d'autres ministères et organismes, les organisations spécialisées, les fournisseurs et autres intervenants techniques, les enquêteurs des forces de l'ordre ou autres organismes chargés d'une enquête, etc. ;
- Valider et compléter les communiqués internes qui concernent les actions réalisées ou à réaliser face aux incidents (alerte, précautions à prendre, rétablissement d'une situation, etc.) ;
- Préparer, au besoin, le rapport pour les incidents à portée gouvernementale ;
- Tenir à jour le registre « Liste des intervenants » et le conserver dans un répertoire aussi accessible par son substitut.

Centre d'assistance en technologies de l'information

Responsable des premières interventions, entre autres pour :

- Résoudre les incidents techniques de premier niveau (ex. virus sur poste de travail) ;
- Déclarer tout incident de sécurité de l'information au COGI ou à son substitut ;
- Collaborer au processus d'escalade.

Autres intervenants

Intervenants internes

Spécialistes en technologies de l'information

Sous la direction du RGTI, des spécialistes en technologies participent aux phases de détection, de réaction et de rétablissement. Ils ont les principales responsabilités suivantes :

- Déployer et installer des systèmes de détection d'intrusion et mettre à jour les vulnérabilités et les règles de filtrage ;
- Mettre en place des outils d'analyse des fichiers de journalisation ;
- Installer et mettre à jour des systèmes d'exploitation, des antivirus, des pare-feu, etc.
- Élaborer et mettre en œuvre des stratégies de confinement des dommages et des procédures d'élimination des sources d'incidents ;
- Valider les prises des copies de sauvegarde et des restaurations ;
- Préserver les preuves ;
- Remettre les systèmes en état à la suite d'un incident ;
- Évaluer les répercussions ;
- Contribuer aux enquêtes ;
- Consigner les incidents.

Utilisateurs des technologies de l'information

L'utilisateur des technologies de l'information est tenu de respecter les règles de sécurité de l'information établies par l'ISQ et donc de déclarer les incidents en sécurité de l'information dont il est témoin, selon la procédure établie par l'ISQ.

Intervenants externes

CERT/AQ

Computer Emergency Response Team de l'Administration québécoise ou *équipe de réponse aux incidents informatiques à l'échelle gouvernementale*, ses principaux objectifs sont de :

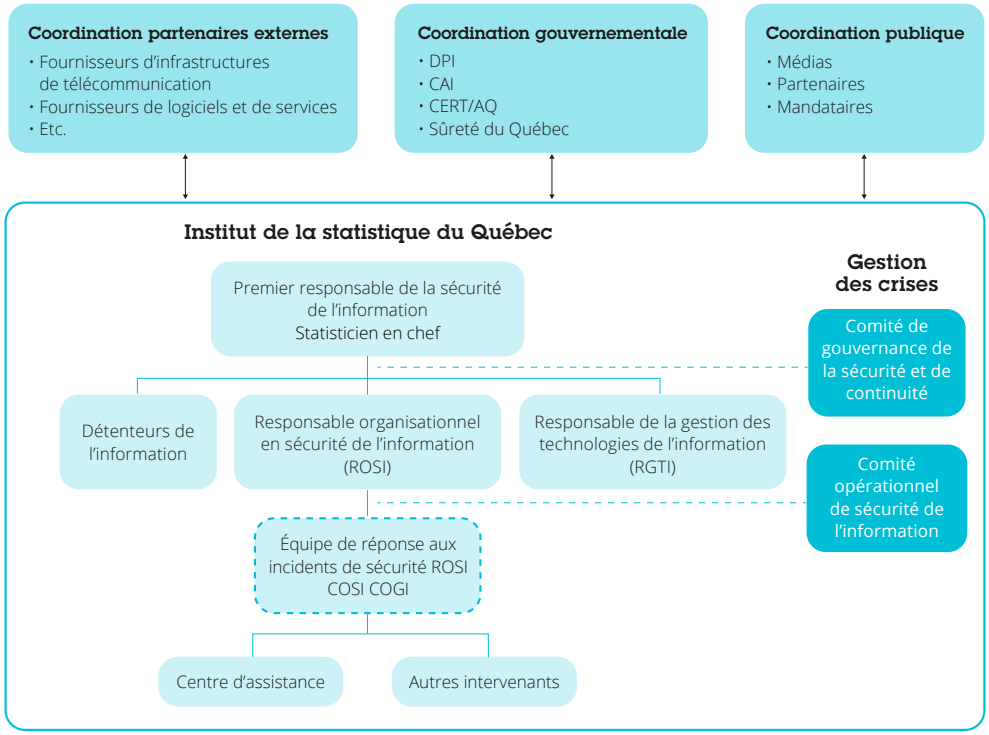
- Assister les ministères et organismes de façon à leur permettre d'améliorer leur capacité à se prémunir contre les incidents de sécurité de l'information et à y faire face, particulièrement les attaques cybernétiques ;
- Coordonner la réaction aux incidents et aux menaces en sécurité de l'information à portée gouvernementale en mettant en relation l'ensemble des spécialistes et en leur fournissant les moyens techniques requis pour un échange efficace d'information, particulièrement en situation de crise.

Autres intervenants externes

L'équipe de réponse peut être appelée à traiter un incident en collaboration avec des fournisseurs de services (Internet, communications, etc.), des fournisseurs de logiciels, des partenaires (ministères et organismes sous ententes), les forces de l'ordre, ou des équipes confrontées à des incidents de même nature.

Structure d'intervention

La figure ci-dessous illustre la structure d'intervention en gestion des incidents en sécurité de l'information. Elle présente l'ensemble des intervenants, tant internes qu'externes, pouvant être appelés à intervenir à diverses étapes du processus de gestion et de traitement des incidents en sécurité de l'information à l'ISQ.



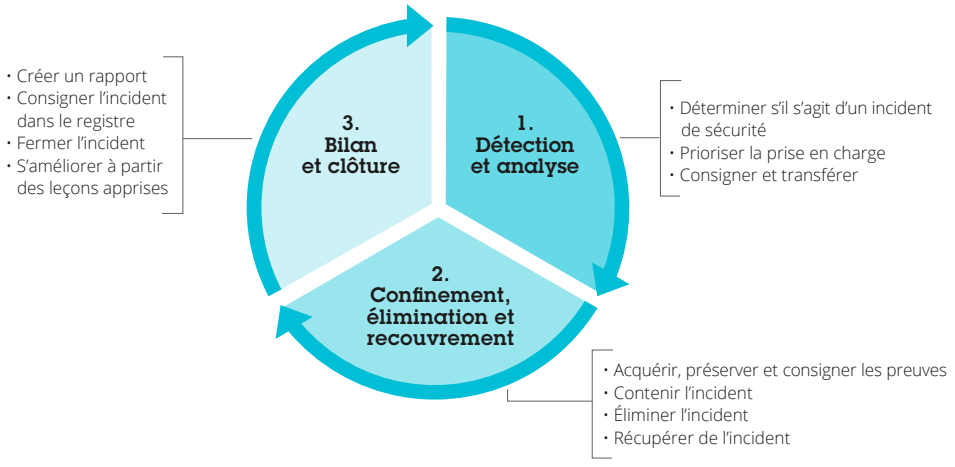
6 Étapes du processus

La présente section décrit les différentes étapes à suivre et les activités à mettre en place en matière de gestion des incidents. Elles sont illustrées à la figure suivante. Elles débutent par la prévention des incidents en sécurité de l'information et se terminent avec le rétablissement des incidents.

La gestion des incidents comporte trois grandes étapes :

Étape	Nom	Description
1	Détection et analyse	Déterminer si la sécurité d'un ou de plusieurs des actifs informationnels de l'organisation a été compromise, et déterminer le niveau de gravité de l'incident.
2	Confinement, élimination et reprise	Prendre en charge l'incident de sécurité, protéger les actifs informationnels de l'organisation et réaliser toutes les activités nécessaires à l'élimination de l'incident jusqu'au retour à la normale. Comprend également les étapes prévues à l'escalade organisationnelle.
3	Bilan et clôture	Consolider l'information sur l'incident et les activités réalisées afin d'améliorer le processus.

La figure suivante illustre l'interrelation des différentes étapes représentées sous la forme d'un cycle de vie :



7 Processus

Le processus de gestion des incidents de sécurité vise à :

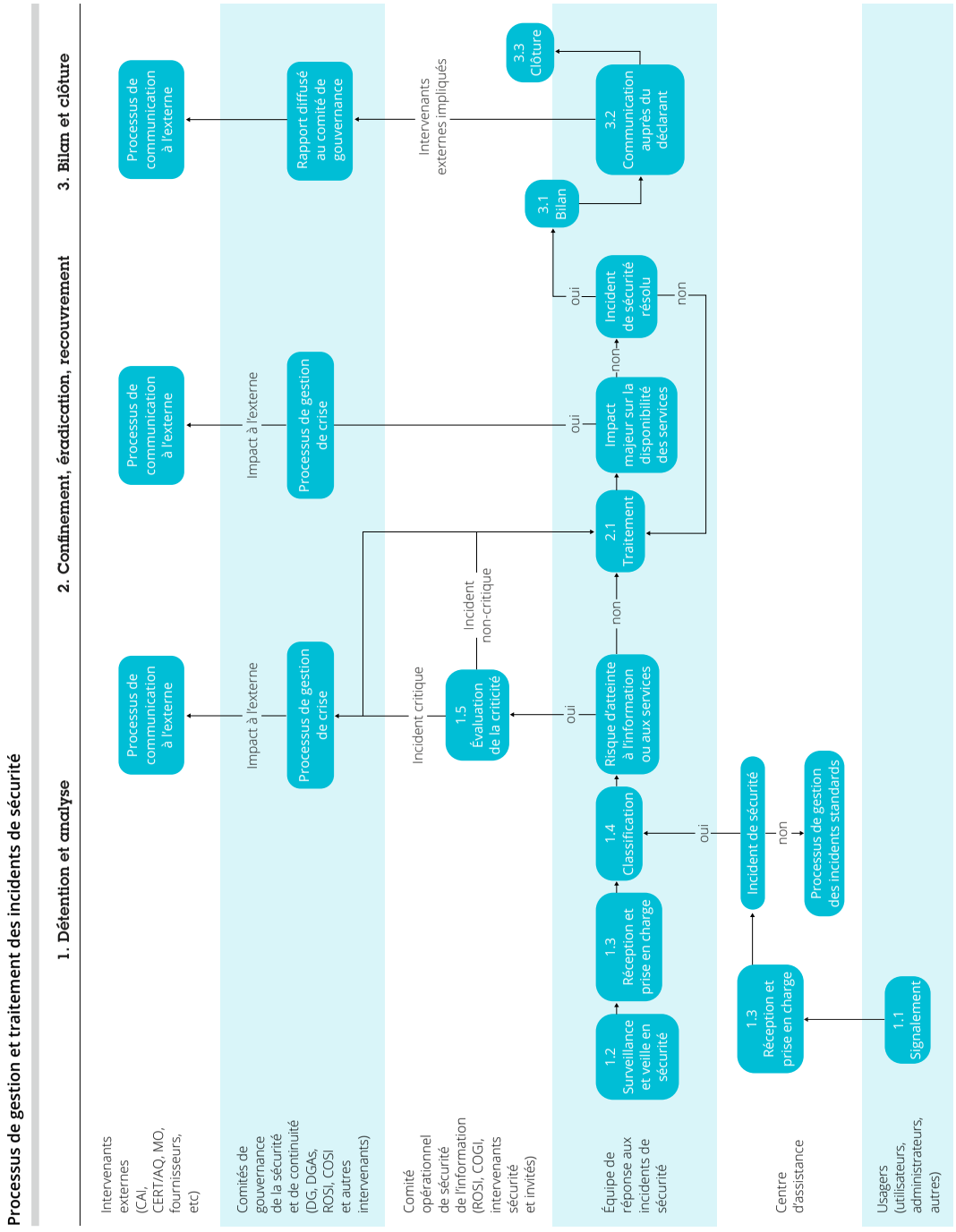
- Assurer une prise en charge des incidents dès qu'ils sont signalés ou dès qu'ils sont détectés grâce à la surveillance et à la veille ;
- Uniformiser le traitement des incidents selon leur type ;
- Classifier tout incident de sécurité ;
- Assurer que les personnes concernées participent à la résolution des incidents ;
- Contenir la source du problème ;
- Appliquer la solution adéquate en fonction de la gravité des incidents ;
- Assurer un suivi auprès des personnes qui signalent les incidents et avec la clientèle concernée ;
- Tirer des conclusions de la résolution des incidents.

Chacune des activités principales du processus se décompose en sous-activités, qui sont décrites dans la section qui suit.

Le présent chapitre détaille les processus de traitement de chacune des catégories d'incident ainsi que les rôles et les responsabilités des différents intervenants.

Il est important de mentionner que la coordination et la communication doivent être effectuées tout au long du processus, selon la nature et le niveau de gravité de l'incident de sécurité.

Le schéma de la page suivante illustre les principales activités du processus.


Processus de gestion et traitement des incidents de sécurité
1. Détention et analyse
2. Confinement, éradication, recouvrement
3. Bilan et clôture
Intervenants externes (CAI, CERT/AQ, MO, fournisseurs, etc)
Comités de gouvernance de la sécurité et de continuité (DG, DGAs, ROSi, COSI et autres intervenants)
Comité opérationnel de sécurité de l'information (ROSI, COGI, intervenants sécurité et invités)
Équipe de réponse aux incidents de sécurité
Centre d'assistance
Usagers (utilisateurs, administrateurs, autres)
1.1 Signalement
1.2 Surveillance et veille en sécurité
1.3 Réception et prise en charge
1.3 Réception et prise en charge
1.4 Classification
Incident de sécurité
Processus de gestion des incidents standards
oui
non
1.5 Évaluation de la criticité
Incident critique
Incident non-critique
Risque d'atteinte à l'information ou aux services
oui
non
Impact à l'externe
Processus de gestion de crise
Processus de communication à l'externe
2.1 Traitement
Impact majeur sur la disponibilité des services
oui
non
Incident de sécurité résolu
oui
non
3.1 Bilan
3.2 Communication auprès du déclarant
3.3 Clôture
Intervenants externes impliqués
Rapport diffusé au comité de gouvernance
Processus de communication à l'externe

Étapes

1. Détection et analyse

1.1 Signalement

Il s'agit du signalement d'un incident de sécurité par un utilisateur, soit toute personne interne ou externe à l'organisation qui constate la présence d'un incident de sécurité et en avise l'organisation.

Procédure de signalement :

- Utilisateurs internes : signalement auprès du centre d'assistance.
- Utilisateurs externes : signalement au service à la clientèle ou au chargé de projet ou aux gestionnaires de l'entente avec un ministère ou organisme, qui contactera le centre d'assistance.

1.2 Surveillance et veille en sécurité

La surveillance et la veille en sécurité sont réalisées par l'équipe de réponse. Un incident est détecté à l'aide des solutions de surveillance en place à différents niveaux de l'environnement technologique ou d'une observation directe par la veille technologique ou tout autre moyen.

Les incidents sont détectés notamment grâce aux actions de surveillance suivantes :

- Surveiller de manière proactive des indicateurs touchant le réseau, les intrusions (IDS) ou les fonctions de veille technologique ;
- Noter les événements et les informations reliés aux indicateurs d'un potentiel incident de sécurité ;
- Analyser les indicateurs surveillés en vue de détecter une activité notable qui pourrait représenter un risque pour l'organisation.

1.3 Réception et prise en charge

La première action consiste à ouvrir un billet et y noter toutes les informations nécessaires à la prise en charge de l'incident telles que :

- Description de l'incident ;
- Systèmes et fonctions affectés ;
- Clientèle visée ;
- Pièces jointes et autres informations complémentaires ;
- Ressources concernées et personnes-ressources ;
- Niveau préliminaire de gravité de l'incident.

Après analyse et vérification des informations reçues, si l'incident n'est pas en lien avec la sécurité, il est relayé au processus de gestion des incidents standards. Autrement, il passe à l'étape de classification.

1.4 Classification

Cette activité très importante vise à établir le type d'incident de sécurité et à évaluer sa sévérité et ses répercussions possibles sur l'organisation. La collecte des informations et la précision de l'évaluation sont primordiales.

1.4.1 Établissement du type d'incident de sécurité

Cette étape a pour objectif de regrouper les incidents selon des groupes prédéfinis en vue de faciliter leur analyse, de préparer la remédiation et de produire des statistiques.

Les types d'incidents sont définis en fonction des procédures techniques de remédiation. Elles sont décrites dans le tableau de la page suivante.

Après l'étape d'identification du type d'incident de sécurité, s'il s'avère qu'il ne s'agit pas d'un incident de sécurité, l'incident est transféré au processus de gestion des incidents standards.

Types d'incidents de sécurité	Définition
Ingénierie sociale	Manipuler et piéger quelqu'un en vue de lui soutirer des informations (ex. un mot de passe ou des informations financières) utilisables pour attaquer des systèmes ou des réseaux.
Hameçonnage	Tenter d'obtenir des informations sensibles (ex. des identifiants et des mots de passe de clients) auprès de clients en se faisant passer pour une personne ou une organisation légitime et de confiance.
Accès non autorisés	Accéder physiquement ou logiquement à un réseau, à un système, à une application, à des données ou à d'autres ressources informatiques, sans autorisation.
Déni de service	Empêcher ou perturber l'utilisation autorisée de réseaux, de systèmes ou d'applications en épuisant les ressources.
Attaque par code malveillant	Infecter ou menacer d'infecter (à grande échelle) par un virus, un ver informatique, un cheval de Troie ou toute autre entité malveillante à base de code informatique.
Rançongiciel	Restreindre l'accès au système informatique qu'on infecte et réclamer une rançon en contrepartie de la levée de la restriction d'accès. Certaines formes de rançongiciels chiffrent les fichiers sur le disque dur du système, alors que d'autres verrouillent simplement le système et affichent un message pour persuader l'utilisateur de payer la rançon demandée.
Usage inapproprié	Incident impliquant un employé interne ou un sous-traitant violant un code de conduite ou une politique informatique. Un comportement inapproprié n'est pas toujours malveillant ou ciblé. Parfois, un utilisateur agira simplement de manière imprudente ou ignorera purement et simplement qu'il a enfreint une politique ou un code de conduite. Le comportement inapproprié constituera parfois un incident de sécurité grave en soi, mais il peut également être la cause ou le déclencheur d'un autre incident grave (ex. infection par un programme malveillant, perte de données critiques).
Fraude	Type de comportement inapproprié malveillant par nature et visant un enrichissement personnel par le détournement de systèmes, d'applications ou d'informations.
Perte ou vol de données	Incident impliquant la perte ou le vol d'informations confidentielles. Une information peut être confidentielle en raison de sa valeur pour l'organisation ou parce qu'elle est protégée par des lois et des règlements internes ou externes. Les incidents liés à une perte de données peuvent avoir des conséquences financières importantes en raison de la responsabilité financière ou des atteintes possibles à l'image de la société si l'information elle-même ou le fait qu'elle ait été perdue est rendu public ou porté à la connaissance des mauvaises personnes.
Détournement de marque	Détourner l'appellation de l'ISQ et de ses travaux déposés.

1.4.2 Évaluation de la sévérité et des répercussions de l'incident de sécurité sur l'organisation

Cette étape consiste à évaluer la sévérité et les répercussions de l'incident de sécurité sur l'information et les services de l'organisation et la clientèle.

Les répercussions sur l'information sont déterminées à partir du tableau ci-dessous.

Répercussions sur l'information	Définition
Aucune	Aucune information n'a été exfiltrée, modifiée, supprimée ou compromise.
Information privée	Des informations sensibles appartenant à l'organisation ont été consultées ou exfiltrées. Aucune répercussion constatée sur les opérations.
Information confidentielle	Des informations confidentielles et stratégiques appartenant à l'organisation, mais n'ayant pas d'incidence sur des citoyens ou des entreprises, ont été consultées ou exfiltrées.
Renseignements personnels	Des informations nominatives et des renseignements personnels ayant une incidence sur des citoyens ou des entreprises ont été consultés ou exfiltrés.

Les répercussions sur les services sont déterminées à partir du tableau ci-dessous.

Répercussions sur les services	Définition
Aucune	Aucun effet sur la capacité de l'organisation à fournir tous ses services à l'ensemble de ses utilisateurs.
Faibles	L'organisation peut encore fournir tous ses services essentiels à l'ensemble de ses utilisateurs, mais a perdu de l'efficacité.
Modérées	L'organisation est incapable de fournir un service critique pour une partie de sa clientèle.
Élevé	L'organisation n'est plus en mesure de fournir des services essentiels à l'ensemble de ses clients.

Note : Il est possible que la gravité de l'incident soit revue à cette étape.

1.5 Analyse de la gravité

Après l'analyse de la sévérité et des répercussions sur l'organisation réalisée à l'étape 1.4.2, l'équipe de réponse transfère l'incident de sécurité au comité opérationnel de la sécurité de l'information aussitôt qu'il y a un risque qui menace l'information et les services de l'organisation et la clientèle.

Par la suite, le comité opérationnel de la sécurité de l'information analyse l'incident et confirme s'il est critique ou non. Dans le cas d'un incident critique, le ROSI décide si le processus de gestion de crise doit être enclenché. Ce processus consiste à convoquer les comités de gouvernance ainsi que les divers intervenants et, au besoin, le comité de continuité des services dont les rôles consistent essentiellement à décider des actions appropriées, à gérer l'information et à assurer une communication adéquate à l'interne et à l'externe.

2. Confinement, élimination et reprise

2.1 Traitement

Cette activité comporte trois étapes : préparation de l'équipe de réponse, évaluation du délai de recouvrement et confinement, élimination et reprise.

2.1.1 Préparation de l'équipe de réponse à l'incident de sécurité

Le succès du traitement de l'incident passe par la préparation de l'équipe. Les critères de succès sont les suivants :

- Assigner un responsable de l'équipe ;
- Assigner et mobiliser les ressources nécessaires ;
- Faciliter la communication et le partage d'information.

2.1.2 Évaluer le délai de reprise

Cette étape consiste à évaluer le délai de reprise dans le but de déterminer s'il y a des répercussions sur la disponibilité des services et si des ressources supplémentaires sont nécessaires.

Le tableau suivant sert à l'évaluation du délai de reprise :

Reprise	Délai
Normal	Prévisible avec les ressources existantes.
Ressources supplémentaires	Prévisible avec des ressources supplémentaires.
Aide extérieure	Imprévisible, nécessite des ressources supplémentaires et une aide extérieure.

2.1.3 Confinement, élimination et reprise

Cette étape comporte plusieurs tâches qui diffèrent selon le type d'incident de sécurité. L'important est de :

- Confiner l'incident de sécurité afin de réduire sa propagation tout en conservant les preuves nécessaires à la conduite d'une enquête ;
- Éliminer totalement l'incident de sécurité et veiller à ce qu'il ne réapparaisse pas ;
- Rétablir les systèmes et les informations en vue d'un retour à la normale.

Se référer aux procédures techniques de réponse aux incidents[2] pour intervenir de façon spécifique à chaque incident. S'assurer que le billet est continuellement alimenté et contient toutes les informations pertinentes.

Tout au long de cette étape, évaluer s'il y a un risque sur la disponibilité des services et, le cas échéant, escalader au comité opérationnel de la sécurité de l'information, qui escaladera à son tour selon la sévérité et les circonstances.

3. Bilan et clôture

3.1 Bilan

Cette activité comporte deux étapes : réaliser un atelier de bilan et alimenter le registre des incidents de sécurité.

3.1.1 Réaliser un atelier de bilan

Les intervenants ayant participé à la résolution de l'incident se réunissent afin de s'assurer qu'ils ont toute l'information et échangent sur l'incident dans son ensemble. Le COGI est responsable de l'atelier de bilan et de la consignation du bilan au moyen du gabarit en annexe.

Le bilan doit répondre, entre autres, aux questions suivantes :

- Quelles étaient la nature exacte et la cause de l'incident ?
- L'incident aurait-il pu être évité ? Si oui, comment ?
- Le personnel ayant participé au processus a-t-il agi de façon adéquate aux différentes étapes ?
- Les échéanciers ont-ils été respectés ?
- La documentation nécessaire à la réponse d'incident était-elle immédiatement disponible ? Était-elle pertinente ?
- Quel fut le coût de l'incident ?
- Comment pourrait-on améliorer le Processus de gestion et de traitement des incidents en sécurité de l'information dans son ensemble ?

Le bilan doit être soumis au ROSI pour approbation, puis ajuster en fonction de ses commentaires.

3.1.2 Alimenter le registre des incidents de sécurité

Pour chaque incident de sécurité, le COGI est chargé d'alimenter le registre des incidents de sécurité à l'aide du gabarit en annexe.

2. Procédure de traitement des incidents, juin 2016.

3.2 Communication auprès de la clientèle

Dans le cas d'un incident de sécurité impliquant la clientèle, le processus de communication à l'externe sert à communiquer avec les intervenants externes concernés et les informer de la résolution de l'incident, conformément aux ententes établies avec la clientèle.

3.3 Clôture

Le comité opérationnel de la sécurité de l'information est responsable de la clôture de l'incident. Il s'assure que toutes les étapes suivantes sont réalisées :

- Solution définitive apportée à l'incident ;
- Rédaction du document de bilan ;
- Inscription au registre des incidents de sécurité.

En terminant, le comité opérationnel de la sécurité de l'information s'assure de consigner l'événement, de mettre en application les améliorations au processus et les recommandations du bilan (ex. sensibilisation, etc.), de faire le suivi et de fermer le billet.

Rôles et responsabilités

Le tableau suivant présente les rôles et responsabilités des acteurs du processus :

#	Activités	Usagers	Centre d'assistance	Équipe de réponse aux incidents en sécurité de l'information	Comité opérationnel de la sécurité de l'information	Comité de gouvernance de la sécurité de l'information[1]	Comité de continuité des services[2]
Détection et analyse							
1.1	Signalement	R	I				
1.2	Surveillance et veille en sécurité			R			
1.3	Réception et prise en charge		R	R			
1.4	Classification		C	R	I		
1.5	Analyse de gravité			C	R	I	
Confinement, élimination et reprise							
2.1	Traitement		C	R	C	I	C/I*
Bilan et clôture							
3.1	Bilan	C	C	C	R	C	C*
3.2	Communication auprès de la clientèle	I				R	C/I*
3.3	Clôture	I	I*	I*	R	I	I*

R Responsable
A Approuve
C Consulté
I Informé
* Au besoin

1. Selon le niveau de gravité, le comité peut inclure les intervenants externes (ministères, organismes, fournisseurs et prestataires de service, CERTAQ, etc.).
2. *Idem*. Ajout du dirigeant principal de l'information (DPI) et de la Commission d'accès à l'information (CAI) le cas échéant.

8 Acronymes et définitions

Acronymes	Définitions
Administrateur	Ressource responsable du fonctionnement et de la maintenance d'un système ou d'un réseau.
Antiprogramme	Programme ou partie de programme destiné à perturber, à altérer ou à détruire, en tout ou en partie, des éléments logiques indispensables au bon fonctionnement d'un système informatique.
Déni de services	Refus ou restriction d'accès aux ressources autorisées d'un système informatique, malgré que le sujet se soit conformé à la procédure d'accès.
ÉRI	Équipe de réponse aux incidents.
Incident de sécurité de l'information	Circonstance au cours de laquelle la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel détenu par l'ISQ a été affectée, de même que toute situation présentant les conditions requises pour qu'un tel résultat se produise.
Plan de continuité de services	Processus assurant le maintien des services essentiels et stratégiques d'une organisation.
Réseau d'alerte	Espace de collaboration gouvernementale favorisant la diffusion d'information technique et le partage d'expertise entre les COGI des ministères et organismes. Le réseau d'alerte vise à améliorer la capacité de l'ensemble des ministères et organismes à se prémunir contre les incidents et les attaques informatiques et à y réagir.
Virus	Programme informatique infectieux inséré dans un système informatique dans le but d'exercer une action nuisible à son environnement.

Annexes

Annexe 1

Gabarit du bilan d'un incident de sécurité

Bilan d'un incident de sécurité

No/Nom de l'incident :	Date du bilan :
Intervenants :	Équipe/Fonction :
1. Résumé de l'incident	
Service(s) touché(s) :	Client(s) touché(s) :
Date/heure du signalement :	Priorité :
Début de la prise en charge :	Fin de l'incident :
Durée de l'incident :	Nombre d'incidents trouvés :
Description de l'incident :	
2. Points forts	
3. Points faibles	
4. Pistes d'amélioration du processus et des activités de résolution d'incident et de prévention	

Annexe 2

Gabarit du registre des incidents de sécurité

Le registre des incidents est consigné à même le système de gestion du centre d'assistance.

Registre des incidents de sécurité

No	Date du signalement (jj/mm/aaaa)	Personne ayant signalé l'incident	Type d'incident	Gravité (répercussions sur l'information et sur les services)	Date de clôture (jj/mm/aaaa)

Annexe 3

Gabarit de déclaration d'incidents de sécurité aux entités externes

Formulaire de déclaration d'un incident au CERT/AQ

Un incident peut être déclaré sur l'extranet du site Web du CERT/AQ.

Ce site est réservé à l'usage des coordonnateurs organisationnels de gestion des incidents (COGI) des organismes publics.

S'il y a lieu, un des COGI remplira le formulaire de déclaration des incidents prévu à cet effet.

Pour connaître le nom des personnes titulaires de responsabilités en matière de sécurité, consultez la section *Responsabilités* de la page intranet *Sécurité de l'information*.

Formulaire de déclaration d'un incident à la CAI

Pour un incident de sécurité de l'information impliquant des renseignements personnels

La Commission d'accès à l'information (CAI) invite les organismes publics et les entreprises à lui déclarer les incidents de sécurité de l'information impliquant des renseignements personnels dont ils ont été victimes.

Pour ce faire, la CAI met à disposition le formulaire de déclaration d'un incident de sécurité de l'information portant atteinte à des renseignements personnels.

Plus d'informations à ce sujet : cai.gouv.qc.ca/incident-de-securite-impliquant-des-renseignements-personnels/.

Références bibliographiques

Les références ci-dessous ont été utilisées dans le cadre de la rédaction de ce document.

Gouvernement du Québec – Cadre de gestion des risques et des incidents à portée gouvernementale section 3.3.1. [tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_risques_incidents.pdf]

Gendarmerie royale du Canada (GRC) – Guide à l'intention des intervenants en cas d'incident de sécurité informatique. [rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/g2-008-fra.pdf]

ISO/IEC 27035 – Information security incident management. [iso.org/iso/catalogue_detail ?csnumber=44379]

National Institut Standards and Technology (NIST) SP-800-61 – Computer Security Incident Handling Guide (revision 2). [nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf]

National Institut Standards and Technology (NIST) SP800-83 – Guide to Malware Incident Prevention and Handling. [csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf]

SANS Institute – Security Incident Handling in Small Organizations. [sans.org/reading_room/whitepapers/incident/security-incident-handling-small-organizations_32979]

Microsoft – Responding to IT Security Incidents. [technet.microsoft.com/en-us/library/cc700825.aspx]

Carniegie Mellon Software Engineering Institute – Handbook for Computer Security Incident Response Teams (CSIRTs). [resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf]

European Network and Information Security Agency (ENISA) – Good Practice Guide for Incident Management (2010). [enisa.europa.eu/publications/good-practice-guide-for-incident-management]

European Network and Information Security Agency (ENISA) – Cadre d'évaluation des capacités nationales (2020). [enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-fr.pdf]

« La statistique au
service de la société :
la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec

Annexe 8

Institut de la statistique Québec

Demande d'accès aux données de recherche

Institut de la statistique Québec

OBJET DE LA DEMANDE

Numéro de la demande	-
Titre officiel du projet	
Date de soumission de la demande	-
Type de demande	Demande d'accès aux données

Institut de la statistique Québec

IDENTIFICATION

Nom		**Prénom**	
Nom de l'organisme, de l'université ou de l'établissement			
Fonction exercée dans l'organisme de rattachement principal			
Courriel principal		**Courriel secondaire**	
		-	
Adresse postale			
Numéro	**Rue**		**Bureau**
Ville	**Province ou état**	**Pays**	**Code postal**
Téléphone(s)			
Numéro	**Type**		
Curriculum vitæ (optionnel)			
Preuve d'affiliation			

Institut de la statistique Québec

DESCRIPTION DU PROJET DE RECHERCHE

Nom du projet
Titre officiel du projet
Titre long du projet
Titre abrégé du projet
Titre court
Description du projet (introduction et problématique)
Description
Population à l'étude
Description générale de la population à l'étude
Description de la population
Objectif principal et objectifs secondaires du projet
Objectif 1 Objectif 2 ...
Méthodologie du projet
Description de la méthodologie (échantillonnage, critères de sélection, etc.)
Étapes de la recherche (optionnel: étapes à préciser dans le cas où des données non désignées doivent être ajoutées)
Étape 1 Étape 2 ...
Protocole de recherche ou description détaillée des activités de recherche
Protocole projet X.docx

3 / 16

Institut de la statistique Québec

Durée désirée de l'accès aux données (entre 1 et 5 ans)

Institut de la statistique Québec

ÉVALUATION ÉTHIQUE

Le projet a-t-il été soumis à un comité d'éthique à la recherche (CÉR) ou a-t-il fait l'objet d'une décision d'un CÉR?	

Comité 1	
Nom du comité d'éthique	
CER établissement X	
Statut de l'évaluation	
Date anticipée de décision	
Commentaire	

5 / 16

Institut de la statistique Québec

ÉQUIPE DE RECHERCHE

Membre 1		
Nom	**Prénom**	
Nom de l'organisme, de l'université ou de l'établissement de rattachement principal		
Fonction exercée dans l'organisme de rattachement principal		
Courriel principal	**Téléphone**	**Type de téléphone**
Rôle		
Chercheur(e) principal(e) (signataire du contrat)		
Droits		
Accès aux données Lecture Modification de l'équipe Modification du projet Personne-ressource : communication avec l'ISQ, (réponse aux questions, transmission de documents, etc.)		
Curriculum vitæ (optionnel)	cv.docx	

Institut de la statistique Québec

Membre 2		
Nom	**Prénom**	
Nom de l'organisme, de l'université ou de l'établissement de rattachement principal		
Fonction exercée dans l'organisme de rattachement principal		
Courriel principal	**Téléphone**	**Type de téléphone**
	-	
Rôle		
Droits		
Accès aux données Lecture Modification du projet		
Curriculum vitæ (optionnel)		

Institut de la statistique Québec

COMMISSION D'ACCÈS À L'INFORMATION (CAI)

Le projet a-t-il été évalué par la CAI?	
Si oui, veuillez fournir les autorisations émises antérieurement.	

Cette section sert à donner l'historique des autorisations CAI dans les cas suivants: demande de modification, de prolongation ou d'utilisation secondaire.

8 / 16

Institut de la statistique Québec

FACTURATION

Destinataire de la facturation			
Est-ce que le ou la destinataire de la facturation est le (la) chercheur(e) principal(e)?			
Identification du destinataire			
Nom		**Prénom**	
Nom de l'institution ou de l'établissement			
Téléphone		**Courriel**	
Adresse de facturation			
Numéro	**Rue**		**Bureau**
Ville	**Province ou état**	**Pays**	**Code postal**

9 / 16

Institut de la statistique Québec

DONNÉES DISPONIBLES VIA LE GUICHET

Institut de la statistique Québec

Cohorte : Cohorte fictive (n° 1)	
Nombre d'individus estimé	**Les individus doivent-ils être distincts de ceux des autres cohortes?**
Critères de sélection	
Description générale des critères de sélection	
Description générale des critères de sélection des individus	
Critères de sélection appliqués aux données administratives du ministère de la Santé et des Services sociaux (MSSS)	
Maintenance et exploitation des données pour l'étude de la clientèle hospitalière (MED-ECHO)	
Période des séjours	
Date de référence pour les critères de sélection	Au moment de l'extraction des données
Critère	**Valeur**
Données à extraire	
Extraction de données administratives de la Régie de l'assurance maladie du Québec (RAMQ)	
Fichier d'inscription des personnes assurées (FIPA)	
Période d'extraction	
Date de référence pour les données	

Institut de la statistique Québec

Cohorte : Cohorte fictive (n° 1)	
Renseignements	**Justification**
Numéro banalisé de la personne	-
Année et mois de naissance Âge Groupe d'âge Autre indicateur d'âge	Justification à l'appui, relative aux objectifs
Sexe de la personne	Justification à l'appui, relative aux objectifs
Région sociosanitaire de résidence Pour chaque année dans la période de recherche	Justification à l'appui, relative aux objectifs
Territoire CLSC de la résidence Pour chaque année dans la période de recherche	Justification à l'appui, relative aux objectifs
Code postal de résidence de la personne (3 premières positions) Pour chaque année dans la période de recherche	Justification à l'appui, relative aux objectifs
Date du décès	Justification à l'appui, relative aux objectifs
Admissibilité au régime public d'assurance médicaments	
Période d'admissibilité	
Date de référence pour les données	
Renseignements	**Justification**
Le fichier sur les périodes d'admissibilité à l'assurance médicaments	
Information sur la personne qui reçoit le service · Numéro banalisé de la personne · Code de programme · Code de plan · Année et mois de début d'admissibilité · Année et mois de fin d'admissibilité	Justification à l'appui, relative aux objectifs
Services pharmaceutiques	
Précisions sur les services	
Période de prestation des services	
Date de référence pour les données	
Renseignements	**Justification**
Le fichier sur les services pharmaceutiques	

Institut de la statistique Québec

Cohorte : Cohorte fictive (n^{o} 1)	
Information sur le service · Date du service · Code DIN · Classe AHF · Code de dénomination commune · Code de forme · Code de teneur · Code de nature d'expression d'ordonnance · Code de sélection du médicament · Durée de traitement · Quantité du médicament	Justification à l'appui, relative aux objectifs
Information sur le prescripteur · Classe du prescripteur · Numéro banalisé du prescripteur · Spécialité du prescripteur	Justification à l'appui, relative aux objectifs
Information sur le lieu du service · Numéro banalisé de la pharmacie · Région de prestation des services pharmaceutiques	Justification à l'appui, relative aux objectifs
Information sur le coût du service · Coût total · Contribution du bénéficiaire	Justification à l'appui, relative aux objectifs
Services médicaux rémunérés à l'acte	
Précisions sur les services	
Période de prestation des services	
Date de référence pour les données	
Renseignements	**Justification**
Les renseignements sur les services médicaux rémunérés à l'acte	

13 / 16

Institut de la statistique Québec

Cohorte : Cohorte fictive (n° 1)	
Information sur le service · Code de catégorie d'actes · Code d'acte · Rôle dans l'exécution de l'acte · Date du service · Code de diagnostic · Numéro banalisé de la facture	Justification à l'appui, relative aux objectifs
Information sur le professionnel traitant · Classe du professionnel · Numéro banalisé du professionnel · Spécialité du professionnel · Code d'entente de facturation	Justification à l'appui, relative aux objectifs
Information sur le professionnel référent · Classe du professionnel référent · Numéro banalisé du professionnel référent · Spécialité du professionnel référent	Justification à l'appui, relative aux objectifs
Information sur le lieu du service · Type d'établissement · Code de secteur d'activité · Numéro banalisé du lieu de prestation de soins (établissement) · Code de localité banalisé du lieu de prestation de soins · Région de prestation de soins	Justification à l'appui, relative aux objectifs
Information sur le coût du service · Montant facturé	Justification à l'appui, relative aux objectifs

Institut de la statistique Québec

APPARIEMENT OU JUMELAGE DE DONNÉES

Le projet nécessite-t-il le jumelage avec des fichiers externes au guichet?	

15 / 16

Institut de la statistique Québec

MODALITÉS D'ACCÈS

Logiciel(s) nécessaire(s)	
Lieu(x) d'accès aux données	

« La statistique au service de la société : la référence au Québec »

statistique.quebec.ca

Institut de la statistique Québec