INSTITUT
DE LA STATISTIQUE
DU QUÉBEC

Politique de sécurité de l'information

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 :	

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

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