Ministère
de la Cybersécurité
et du Numérique
Québec

Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques

Statut	En vigueur
Diffusion	Non restreinte
No de référence	IA-SI-2023-001-OP
Organismes visés	Organismes publics
Indication formulée par	Dirigeant principal de l'information
Référence légale	LGGRI, chapitre G-1.03, art. 7
Date de formulation	2023-02-01
Date d'entrée en vigueur	2023-02-01
Date de mise à jour	S. O.
Expiration	Indéterminée

SECTION I
Dispositions introductives

1. La présente indication d'application énonce les mesures minimales de sécurité au regard des données que les organismes publics doivent appliquer lors de l'utilisation de solutions technologiques, que ces solutions soient ou non à portée gouvernementale. Les solutions d'affaires en gestion intégrée des ressources (SAGIR) et le Système automatisé de gestion des informations sur le personnel (SAGIP) sont, à titre d'exemples, des solutions à portée gouvernementale.

Elle s'inscrit, par ailleurs, dans une perspective de protection adéquate pour les renseignements personnels, dans le respect des obligations prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1, ci-après « Loi sur l'accès »).

Elle s'adresse plus particulièrement aux dirigeants de l'information qui se rattachent aux organismes publics.

2. La présente indication d'application 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, ci-après « Loi »).

SECTION II
Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques

§ 1.- Obligation en sécurité de l'information

3. Un organisme public doit, au regard des données lors de l'utilisation de solutions technologiques, appliquer les mesures minimales de sécurité prévues aux sous-sections 2 et 3, dans l'objectif d'assurer la sécurité de l'information tel que le prévoit la Loi et les textes d'application qui la complètent, notamment la Directive gouvernementale sur la sécurité de l'information, approuvée par le décret numéro 1514-2021 du 8 décembre 2021 (2021, G.O. 2, 7694). Ces mesures minimales de sécurité contribueront également au respect de l'article 63.1 de la Loi sur l'accès qui prévoit qu'un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Une pondération dans l'application de telles mesures est permise, lorsque cette pondération est nécessaire en raison de l'application du modèle de classification de sécurité des données numériques gouvernementales visé par le paragraphe 3° du premier alinéa de l'article 12.6 de la Loi.

§ 2.- Mesures de sécurité relatives aux accès

4. Les mesures de sécurité relatives aux accès qu'un organisme public doit appliquer sont les suivantes :

1° mettre en place des mécanismes de contrôle pour les droits d'accès et les privilèges d'accès, en tenant compte du besoin de connaître (les personnes doivent accéder uniquement aux données qui sont nécessaires à l'exercice de leurs fonctions), de la séparation des tâches et du principe de moindre privilège, notamment les mécanismes suivants :

a) un processus d'autorisation et de révocation pour de tels droits et de tels privilèges;

b) un processus de révision périodique, au moins une fois l'an, de tels droits et de tels privilèges;

c) la vérification de la probité des personnes détenant des privilèges d'accès, incluant la vérification des antécédents judiciaires, lorsque la situation le justifie;

2° effectuer une reddition de comptes à intervalles réguliers auprès de la haute direction de son organisation et du chef délégué de la sécurité de l'information qui s'y rattache ainsi qu'auprès du chef gouvernemental de la sécurité de l'information, en appliquant préalablement les mesures de corrections appropriées, le cas échéant.

Le processus prévu au sous-paragraphe *a*) du premier alinéa doit faire en sorte que les privilèges d'accès accordés le soient, autant que possible, à des personnes plutôt qu'à des comptes génériques.

§ 3.- Mesures de sécurité relatives aux données comprenant des renseignements confidentiels, incluant des renseignements personnels

5. Les mesures de sécurité relatives aux données comprenant des renseignements confidentiels, incluant des renseignements personnels, qu'un organisme public doit appliquer sont les suivantes :

1° établir un processus permettant d'appliquer, pour chaque service d'un tel organisme, au cas par cas, le principe de minimisation consistant en :

a) une réduction au minimum de la collecte de telles données, c'est-à-dire de collecter uniquement les données nécessaires en lien avec les besoins du traitement;

b) la prise en compte de ce principe dès la conception de la solution technologique liée à un service d'un tel organisme et tout le long de la phase d'exploitation de celle-ci;

c) une réduction au minimum du temps de conservation de telles données, c'est-à-dire que les données doivent être détruites dès que les fins pour lesquelles elles ont été recueillies ou utilisées sont accomplies, sous réserve d'exigences légales;

2° établir un processus de supervision des actions concernant l'accès à de telles données et l'utilisation de ces accès tels que le téléchargement ou l'impression, notamment par la surveillance et par la journalisation;

3° établir des principes de conduite au regard des opérations d'extraction et de la communication de telles données et diffuser ces principes avec diligence aux personnes concernées;

4° privilégier l'anonymisation des renseignements personnels ou, à défaut, l'utilisation de ceux-ci sous une forme ne permettant pas d'identifier directement la personne concernée par ceux-ci;

5° indiquer les configurations de sécurité à être appliquées à de telles données, notamment les chiffrer avec un algorithme de chiffrement répondant à une norme reconnue et adéquate considérant leur degré de sensibilité;

6° s'assurer, dans le cadre de la réalisation d'un projet en ressources informationnelles, de privilégier les données fictives plutôt que les données réelles;

7° établir des procédures de conservation de telles données lorsque celles-ci sont extraites, notamment en imposant le recours à des supports verrouillés et/ou des lieux sécurisés;

8° établir des procédures relatives à la destruction et à l'effacement complet et permanent de telles données, en privilégiant autant que possible l'effacement cryptographique ou l'application de normes reconnues pour nettoyer les dispositifs et le déchiquetage de tout dispositif physique en fin de vie;

9° s'assurer de développer et de maintenir, auprès des membres de son personnel, des compétences en matière de sécurité de l'information et, le cas échéant, de protection des renseignements personnels au regard de telles données.

Les mesures prévues au premier alinéa s'appliquent, avec les adaptations nécessaires, au regard des données comprenant des renseignements confidentiels, incluant des renseignements personnels, qui sont portées par un support papier ou tout autre support, même après leur extraction à partir d'une solution technologique.

Indications d'application liées (s'il y a lieu) :

- IA-SI-2020-004-OP « Authentification multifacteur (« MFA ») pour les accès réalisés à partir d'Internet »
- IA-SI-2020-006-OP « Sécurisation des courriels pour les échanges de données sensibles »
- IA-SI-2020-008-OP « Surveillance continue des authentifications »
- IA-SI-2020-014-OP « Gestion des accès employés »

Mots-clés : mesures minimales de sécurité | identification | authentification | données | solutions technologiques | SAGIP | SAGIR | protection | renseignements personnels | dirigeants de l'information | sécurité de l'information | classification des données | destruction |

Une indication d'application est une instruction donnée par écrit portant sur l'exécution d'activités, l'acquittement de responsabilités ou l'application de mesures en matière de ressources informationnelles, à laquelle les organismes publics doivent se conformer en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).