Décret 7-2014 du 15 janvier 2014

DIRECTIVE SUR LA SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, chapitre G-1.03, a. 20

OBJET

1. La présente directive a pour objet d'assurer la sécurité de l'information qu'un organisme public détient dans l'exercice de ses fonctions, que la conservation de cette information, ci-après appelée l'information gouvernementale, soit assurée par lui-même ou par un tiers.

   Elle fixe les objectifs à atteindre, énonce les principes directeurs devant être appliqués et établit les obligations du dirigeant principal de l'information et des organismes publics pour assurer la sécurité de l'information gouvernementale tout au long de son cycle de vie. Elle est appuyée par un cadre gouvernemental de gestion de la sécurité de l'information, un cadre de gestion des risques et des incidents à portée gouvernementale et une approche stratégique triennale 2014-2017 de sécurité de l'information.

CHAMP D'APPLICATION

2. 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), ci-après appelée la Loi.

DÉFINITIONS

3. Dans la présente directive, nous entendons par :

a) **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.

b) **Détenteur de l'information :** un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

c) **Document :** un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrits sous l'une de ces formes ou en un autre système de symboles.

Est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

d) **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 et 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 au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

e) **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, nécessitant une intervention concertée au plan gouvernemental.

f) **Services communs de sécurité de l'information :** services utilisés par plusieurs organismes publics et dont la gestion est centralisée.

OBJECTIFS ET PRINCIPES DIRECTEURS DE LA SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

4. Les mesures de sécurité doivent être proportionnelles à la valeur de l'information gouvernementale à protéger. Elles sont établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences. Plus particulièrement, ces mesures visent à :

a) Assurer la disponibilité de l'information gouvernementale de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée.

b) 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.

c) Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité.

d) Permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.

e) 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.

5. Les organismes publics doivent assurer la sécurité de l'information gouvernementale conformément aux principes directeurs suivants :

a) **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 de comptes adéquate.

b) **Évolution :** 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.

c) **Universalité :** 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.

d) **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.

OBLIGATIONS DU DIRIGEANT PRINCIPAL DE L'INFORMATION

6. Le dirigeant principal de l'information conseille le Conseil du trésor dans sa fonction de gouverne de la sécurité de l'information gouvernementale et fournit aux organismes publics les outils et l'assistance leur permettant de prendre en charge les exigences s'y rapportant. À cette fin, il doit :

a) Déposer au Conseil du trésor :

i) Un rapport sur l'état de situation gouvernemental de sécurité de l'information, au plus tard le 30 novembre 2014 et, par la suite, selon une périodicité bisannuelle à compter de cette date. Ce rapport indique le bilan gouvernemental en cette matière en date du 31 mars précédent.

ii) Un rapport sur les risques de sécurité de l'information à portée gouvernementale, au plus tard le 31 octobre de chaque année, et ce, à compter de 2014. Ce rapport indique l'état de situation en cette matière en date du 31 mars précédent.

b) Proposer au Conseil du trésor un cadre gouvernemental de gestion de la sécurité de l'information, un cadre de gestion des risques et des incidents à portée gouvernementale et une approche stratégique triennale de sécurité de l'information.

c) Mettre en place les instances de concertation gouvernementales, en matière de sécurité de l'information, décrites dans le cadre gouvernemental de gestion de la sécurité de l'information, et en assurer la coordination.

d) Mettre en place un registre des responsables organisationnels de la sécurité de l'information, et en assurer la gestion.

e) Mettre en œuvre, conjointement avec l'Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise, relevant du Centre de services partagés du Québec et ci-après appelée le CERT/AQ, un processus de gestion des incidents à portée gouvernementale.

f) Proposer au Conseil du trésor les services communs de sécurité de l'information, leurs composantes, ainsi que les procédures et les règles de gestion associées.

OBLIGATIONS GÉNÉRALES DES ORGANISMES PUBLICS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Gouvernance et gestion de la sécurité de l'information

7. Le sous-ministre ou le dirigeant d'un organisme public, visé à l'un des paragraphes 1º à 3º ou 6º du premier alinéa de l'article 2 ou, le cas échéant, à l'article 3 de la Loi, doit, en prenant appui sur les orientations et les bonnes pratiques gouvernementales en matière de sécurité de l'information :

a) 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.

b) Déposer au dirigeant principal de l'information, selon les modalités et le format fixés par ce dernier :

i) Une planification des actions de sécurité de l'information au plus tard le 31 mai 2014 et, par la suite, selon une périodicité bisannuelle à compter de cette date. Cette planification inclut les priorités d'action et les échéanciers afférents découlant des exercices d'audits et de tests d'intrusion.
ii) Un bilan de sécurité de l'information au plus tard le 31 mai 2014 et, par la suite, selon une périodicité bisannuelle à compter de cette date.

c) S'assurer de la mise en œuvre des processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

d) Déclarer au dirigeant principal de l'information, selon les modalités fixées par ce dernier, les risques de sécurité de l'information à portée gouvernementale.

e) Déclarer au CERT/AQ, selon les modalités fixées par ce dernier, les incidents de sécurité de l'information à portée gouvernementale.

f) S'assurer de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents.

g) S'assurer de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégager les priorités d'actions et les échéanciers afférents.

h) S'assurer de la mise en place d'un registre d'autorité de la sécurité de l'information. Sont notamment consignés, dans ce registre, les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

i) 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.

j) Favoriser l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor.

k) Définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.

Le ministre de l'Éducation, du Loisir et du Sport, le ministre de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie et le ministre de la Santé et des Services sociaux, appuyés par les dirigeants réseaux de l'information, doivent s'assurer que les organismes publics visés aux paragraphes 4°et 5° du premier alinéa de l'article 2 de la Loi respectent les obligations prévues au premier alinéa.

Les documents produits par ces organismes publics, en application du paragraphe b) du premier alinéa, doivent être transmis au dirigeant réseau de l'information, auquel ils sont rattachés, pour que celui-ci en fasse une synthèse et la dépose auprès du dirigeant principal de l'information, au plus tard le 30 septembre 2014, et, par la suite, selon une périodicité bisannuelle à compter de cette date. La démarche est la même pour les obligations prévues aux paragraphes d) et e) du premier alinéa.

Désignation des principaux intervenants en sécurité de l'information

8. Le sous-ministre ou le dirigeant d'un organisme public, visé à l'un des paragraphes 1º à 3º ou 6º du premier alinéa de l'article 2 ou, le cas échéant, de l'article 3 de la Loi, doit :

a) Désigner un responsable organisationnel de la sécurité de l'information pour le représenter en matière de sécurité de l'information auprès de son organisation et auprès du dirigeant principal de l'information. Ce responsable doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur.

b) Désigner un coordonnateur organisationnel de gestion des incidents pour le représenter auprès du réseau d'alerte gouvernemental et y participer activement. Ce coordonnateur doit être un employé régulier de l'organisme public et appartenir à la classe d'emploi de niveau professionnel ou à une classe d'emploi de niveau supérieur.

Les rôles et les responsabilités de ces principaux intervenants en sécurité de l'information sont décrits dans le cadre gouvernemental de gestion de la sécurité de l'information.

Malgré le premier alinéa, un organisme public peut prendre entente avec un autre organisme public relevant du même ministre afin que le responsable organisationnel de la sécurité de l'information ou le coordonnateur organisationnel de gestion des incidents de l'autre organisme public agisse pour son compte.

Le ministre de l'Éducation, du Loisir et du Sport, le ministre de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie et le ministre de la Santé et des Services sociaux, selon les mêmes conditions énoncées au premier alinéa, doivent désigner un responsable organisationnel de la sécurité de l'information et un coordonnateur organisationnel de gestion des incidents pour les représenter en matière de sécurité de l'information auprès de leurs réseaux respectifs et, selon le cas, auprès du dirigeant principal de l'information ou du réseau d'alerte gouvernemental.

OBLIGATIONS PARTICULIÈRES DU CENTRE DE SERVICES PARTAGÉS DU QUÉBEC ET DU CONTRÔLEUR DES FINANCES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Le Centre de services partagés du Québec

9. Par l'entremise du CERT/AQ, le Centre de services partagés du Québec doit :

   a) Présenter au dirigeant principal de l'information, conjointement avec le ministère de la Sécurité publique et la Sûreté du Québec, au plus tard le 30 septembre de chaque année, un rapport sur les incidents de sécurité de l'information à portée gouvernementale déclarés au cours de l'exercice terminé le 31 mars précédent.

   b) Agir à titre de détenteur du registre des coordonnateurs organisationnels de gestion des incidents et du registre des incidents de sécurité de l'information, et en assurer la gestion.

   c) Informer le dirigeant principal de l'information de tout incident de sécurité de l'information à portée gouvernementale.

Le Contrôleur des finances

10. Le Contrôleur des finances veille à l'intégrité du système comptable du gouvernement et s'assure de la fiabilité des données qui y sont enregistrées. À ce titre, il informe, le cas échéant, le dirigeant principal de l'information des situations ayant des incidences sur la sécurité de l'information gouvernementale.

DISPOSITIONS FINALES

11. Le dirigeant principal de l'information, de concert avec les organismes publics, doit présenter au Conseil du trésor une évaluation de l'application de cette directive au plus tard cinq années après son approbation.

12. La présente directive remplace la Directive sur la sécurité de l'information gouvernementale adoptée par la décision du Conseil du trésor du 11 avril 2006.

13. La présente directive entre en vigueur le 15 janvier 2014.