DIRECTIVE GOUVERNEMENTALE SUR LA SÉCURITÉ DE L'INFORMATION

Votre gouvernement

Québec

Cette publication a été réalisée
par le Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information
au sujet du Conseil du trésor et de son secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
du ministère du Conseil exécutif
et du Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158
Courriel : communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

La Directive gouvernementale sur la sécurité de l'information
a été approuvée par le décret numéro 1514-2021 du 8 décembre 2021.
Elle remplace la Directive sur la sécurité de l'information gouvernementale
approuvée par le décret numéro 7-2014 du 15 janvier 2014.

En cas de disparité
entre les informations présentées dans ce document
et celles du recueil des politiques de gestion,
ces dernières ont préséance et sont applicables.

DIRECTIVE GOUVERNEMENTALE SUR LA SÉCURITÉ DE L'INFORMATION

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

SECTION I
OBJET, DÉFINITIONS ET CHAMP D'APPLICATION

1. La présente directive 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.

Par la mise en place d'un encadrement optimal et par l'établissement de règles, elle complète les dispositions de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), en cohérence avec la politique gouvernementale en matière de sécurité de l'information en vigueur, incluant toute modification à celle-ci, afin de viser une Administration publique résiliente et cyberprotégée à l'ère du numérique.

Elle énonce les principes directeurs devant être appliqués et prévoit une gouvernance de la sécurité de l'information qui repose sur une structure de coordination, de concertation et de soutien aux organismes publics en telle matière.

Elle prévoit des règles applicables aux organismes publics en vue d'assurer, en matière de sécurité de l'information, la confidentialité, l'intégrité et la disponibilité de l'information tout au long de son cycle de vie, et afin de couvrir des enjeux particuliers en telle matière.

Elle est appuyée par un cadre gouvernemental de gestion de la sécurité de l'information et des cadres de gestion particuliers en sécurité de l'information.

2. Dans la présente directive, on entend par :

1° « Centre gouvernemental de cyberdéfense » l'unité administrative spécialisée en sécurité de l'information visée à l'article 12.5 de la Loi;

2° « Centre opérationnel de cyberdéfense » l'unité administrative spécialisée en sécurité de l'information visée à l'article 9;

3° « chef gouvernemental de la sécurité de l'information » le dirigeant principal de l'information qui agit à ce titre en vertu du paragraphe 1° du premier alinéa de l'article 7.1 de la Loi;

4° « chef délégué de la sécurité de l'information » le dirigeant de l'information qui agit à ce titre en vertu du paragraphe 9.1° du premier alinéa de l'article 10.1 de la Loi;

5° « chef de la sécurité de l'information organisationnelle » un membre du personnel d'encadrement d'un organisme public désigné en vertu de l'article 10 ou, selon le contexte, le chef délégué de la sécurité de l'information;

6° « 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;

7° « événement de sécurité » toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'un organisme public ou d'une personne agissant pour ce dernier;

8° « lien fonctionnel » un rapport entre deux personnes qui, selon le contexte, permet à l'une d'entre elles de formuler un ordre à l'autre, sans qu'il existe un lien hiérarchique entre ces personnes;

9° « Loi » la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);

10° « responsable gouvernemental de cyberdéfense » la personne désignée en vertu du paragraphe 4° du deuxième alinéa de l'article 5;

11° « responsable opérationnel de cyberdéfense » la personne désignée en vertu du paragraphe 3° du deuxième alinéa de l'article 6;

12° « service commun » un service offert ou fourni par un organisme public à plusieurs organismes publics utilisateurs.

3. La présente directive s'applique aux organismes publics visés à l'article 2 de la Loi, lesquels forment l'Administration publique aux fins de la Loi et de la présente directive.

SECTION II
PRINCIPES DIRECTEURS DE LA SÉCURITÉ DE L'INFORMATION

4. Un organisme public doit assurer la sécurité des ressources informationnelles et de l'information qu'il détient ou utilise conformément aux principes fondamentaux énoncés dans la politique gouvernementale en matière de sécurité de l'information en vigueur, incluant toute modification à celle-ci, et aux cinq principes directeurs suivants :

— **Éthique** : le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle;

— **Évolution** : les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement et actualisées afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'information afférents;

— **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 de processus de gestion de la sécurité de l'information permettant une reddition de comptes adéquate;

— **Transparence** : l'information concernant les événements de sécurité, les pratiques et les solutions de sécurité de l'information afférentes doit être communiquée avec fluidité au sein de l'Administration publique, sous réserve du droit applicable;

— **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.

SECTION III
GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

§ 1. — *Chef gouvernemental de la sécurité de l'information*

5. Le chef gouvernemental de la sécurité de l'information assume les responsabilités découlant de la Loi et de ses textes d'application.

À ce titre, les activités liées à ses responsabilités sont notamment les suivantes :

1° recommander au Conseil du trésor un cadre gouvernemental de gestion de la sécurité de l'information, notamment en ce qui concerne l'organisation fonctionnelle de la sécurité de l'information au sein de l'Administration publique en vue d'assurer la cohérence des interventions en matière de sécurité de l'information;

2° 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;

3° diriger le Centre gouvernemental de cyberdéfense, l'opérationnaliser et contribuer à faire évoluer son offre de services;

4° désigner, 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;

5° définir des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information qui permettent notamment d'assurer la gestion des événements de sécurité, la gestion de crise et la gestion de la performance;

6° mettre en place des comités ou des groupes de travail appropriés de concertation gouvernementale en matière de sécurité de l'information et en assurer la coordination;

7° maintenir à jour un registre des chefs délégués de la sécurité de l'information et un registre des chefs de la sécurité de l'information organisationnelle;

8° fournir aux organismes publics l'accompagnement et l'assistance nécessaires aux niveaux stratégique, tactique et opérationnel leur permettant de prendre en charge les exigences de sécurité de l'information, notamment en mettant à leur disposition des outils et des pratiques exemplaires;

9° prendre les mesures requises pour que les organismes publics s'assurent que les membres de leur personnel adoptent des comportements sécuritaires et des pratiques exemplaires en matière de sécurité de l'information et offrent des formations ciblées.

§ 2. — *Chef délégué de la sécurité de l'information*

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

À ce titre, les activités liées à ses responsabilités sont notamment les suivantes :

1° mettre en œuvre un cadre de gouvernance qui régit la sécurité de l'information;

2° diriger le Centre opérationnel de cyberdéfense auquel il se rattache, l'opérationnaliser en demandant, lorsqu'il le juge à propos, la contribution des organismes qui s'y rattachent, et contribuer à faire évoluer l'offre de services de ce centre;

3° désigner, 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;

4° mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité;

5° élaborer, au besoin et dans un souci d'efficacité et de gestion performante des ressources informationnelles, des processus de sécurité de l'information, déployer les mesures y afférentes et assurer le suivi de leur mise en œuvre;

6° apporter le soutien et l'accompagnement requis en matière de sécurité de l'information, notamment par des conseils, des outils, des pratiques exemplaires de sécurité de l'information ainsi que par le développement des compétences et la sensibilisation du personnel affecté en la matière ou par toute autre mesure jugée nécessaire;

7° mettre en place les comités ou les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination.

§ 3. — *Réseau gouvernemental de cyberdéfense*

7. Est institué, au sein de l'Administration publique, le « Réseau gouvernemental de cyberdéfense » dont la mission vise à renforcer les dispositifs de prévention et de réaction à l'égard des cybermenaces. Ce réseau opère sous le commandement et le leadership du responsable gouvernemental de cyberdéfense qui en assure également la coordination et l'amélioration continue.

Ce réseau est formé :

1° du Centre gouvernemental de cyberdéfense par l'intermédiaire du responsable gouvernemental de cyberdéfense;

2° des centres opérationnels de cyberdéfense par l'intermédiaire des responsables opérationnels de cyberdéfense;

3° des organismes publics par l'intermédiaire des chefs de la sécurité de l'information organisationnelle.

8. Le responsable gouvernemental de cyberdéfense et les responsables opérationnels de cyberdéfense forment ensemble un comité du Réseau gouvernemental de cyberdéfense appelé « Cellule de cyberdéfense ».

§ 4. — Centre opérationnel de cyberdéfense

9. 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 ».

Il en est de même pour tout dirigeant d'un organisme public au sens du troisième alinéa de l'article 8 de la Loi qui a son propre dirigeant de l'information en application du deuxième alinéa de cet article.

Le présent article n'a pas pour effet d'empêcher un ministre ou un dirigeant d'un organisme public qui a son propre dirigeant de l'information de conclure une entente de services avec un autre ministre ou un autre dirigeant d'organisme public qui a son propre dirigeant de l'information ayant pour objet le recours au centre opérationnel de cyberdéfense de ce ministre ou de cet autre organisme, dans le respect de l'article 9 de la Loi. En ce cas, les paragraphes 2° et 3º du premier alinéa de l'article 6 ne s'appliquent pas.

§ 5. — Chef de la sécurité de l'information organisationnelle

10. La fonction de chef de la sécurité de l'information organisationnelle doit être créée au sein de chaque ministère et de chaque organisme public. Ce chef assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation.

Cette fonction est assumée par le chef délégué de la sécurité de l'information lorsqu'il s'agit d'un ministère ou d'un organisme public qui a son propre dirigeant de l'information en application de l'article 8 de la Loi. Dans le cas d'un organisme public, autre qu'un ministère, qui ne bénéficie pas de l'autorisation lui permettant d'avoir son propre dirigeant de l'information, le dirigeant d'un tel organisme doit désigner un membre de son personnel d'encadrement pour agir à titre de chef de la sécurité de l'information organisationnelle.

Tout ministre et tout dirigeant d'un organisme public autre qu'un ministère doit s'assurer du maintien d'un lien fonctionnel entre le chef de la sécurité de l'information organisationnelle, le chef délégué de la sécurité de l'information auquel il est rattaché et le chef gouvernemental de la sécurité de l'information, avec les adaptations nécessaires en cas de cumul de fonctions.

§ 6. — Répondants en matière de sécurité de l'information

11. Un dirigeant d'organisme public au sens du troisième alinéa de l'article 8 de la Loi doit désigner, parmi les membres de son personnel, des répondants pour des domaines spécifiques en matière de sécurité de l'information lorsque le chef gouvernemental de la sécurité de l'information le juge nécessaire.

Il doit s'assurer du maintien d'un lien fonctionnel entre ces répondants, le chef de la sécurité de l'information organisationnelle, le chef délégué de la sécurité de l'information auquel il est rattaché et le chef gouvernemental de la sécurité de l'information, avec les adaptations nécessaires.

SECTION IV
OBLIGATIONS EN SÉCURITÉ DE L'INFORMATION

12. Un organisme public, outre les obligations prévues à la Loi ou à l'un de ses textes d'application, doit :

1° adopter et mettre en œuvre une politique et un cadre de gestion de la sécurité de l'information, les maintenir à jour et en assurer leur application;

2° mettre en place les comités et les groupes de travail appropriés de coordination et de concertation en matière de sécurité de l'information;

3° assurer la gestion de la sécurité de l'information, déployer les mesures y afférentes et assurer le suivi de leur mise en œuvre;

4° appliquer les indications d'application que formule le chef gouvernemental de la sécurité de l'information et les indications d'application particulières que formule le chef délégué de la sécurité de l'information auquel il est rattaché;

5° élaborer et mettre en œuvre, pour les membres de son personnel, un programme formel et continu de formation et de sensibilisation en matière de sécurité de l'information;

6° respecter, lorsqu'il utilise un service commun, les exigences de sécurité de l'information qui le concernent;

7° rendre compte à son chef délégué de la sécurité de l'information du respect des obligations en matière de sécurité de l'information et répondre aux demandes que lui formule ce chef à cet égard.

SECTION V
SERVICES COMMUNS

13. Le chef gouvernemental de la sécurité de l'information exécute, en lien avec ses responsabilités et à l'égard des services communs, les activités suivantes :

1° élaborer et mettre en œuvre un cadre gouvernemental de gestion de la sécurité de l'information applicable aux services communs;

2° s'assurer que les mesures de sécurité de l'information, propres à un service commun et celles applicables aux utilisateurs de ce service, répondent aux enjeux de sécurité de l'information et aux risques afférents.

14. Infrastructures technologiques Québec doit assumer, à l'égard d'un service commun qu'il fournit et des organismes publics utilisateurs de ce service, les responsabilités suivantes :

1° déterminer, après consultation des organismes publics utilisateurs d'un service commun, le partage de responsabilités liées aux exigences en matière de sécurité de l'information eu égard à un tel service et effectuer les mises à jour requises;

2° mettre en place les mesures de sécurité de l'information adéquates et propres à assurer la prise en charge des exigences en matière de sécurité de l'information visées au paragraphe 1° qui le concernent;

3° prendre les moyens nécessaires pour rehausser la capacité des organismes publics utilisateurs d'un service commun à prendre en charge les exigences en matière de sécurité de l'information visées au paragraphe 1° qui les concernent et apporter à de tels organismes le soutien et l'accompagnement requis à cet égard;

4° produire, à la demande du chef gouvernemental de la sécurité de l'information, un état de situation démontrant sa conformité avec les obligations prévues aux paragraphes 1° à 3° ainsi que son respect des attentes en matière de sécurité de l'information, des orientations, standards, stratégies, directives, règles et indications d'application pris en matière de sécurité de l'information en vertu de la Loi;

Le partage de responsabilités visé au premier alinéa ou toute mise à jour à celui-ci doit faire l'objet d'une approbation par le chef gouvernemental de la sécurité de l'information préalablement à toute diffusion auprès des organismes publics utilisateurs d'un service commun. Le chef gouvernemental de la sécurité de l'information peut demander à Infrastructures technologiques Québec d'apporter toute modification à ce partage ou à une mise à jour s'il estime cela nécessaire.

Le présent article s'applique, avec les adaptations nécessaires, à tout autre organisme public qui fournit ou entend fournir un service commun.

SECTION VI
ACQUISITIONS GOUVERNEMENTALES

15. Infrastructures technologiques Québec, en ce qui concerne notamment le service de courtier en infonuagique, et le Centre d'acquisitions gouvernementales doivent :

1° s'assurer de prendre les moyens nécessaires pour que les acquisitions en bien ou en services effectuées pour le compte des organismes publics répondent aux besoins de sécurité de l'information exprimés par ces derniers et permettent de réduire les risques en sécurité de l'information, dans le respect des attentes du chef gouvernemental de la sécurité de l'information signifiées à cet égard, des bonnes pratiques relatives à la sécurité de l'information ainsi que des orientations, standards, directives, règles et indications d'application pris en vertu de la Loi;

2° produire à la demande du chef gouvernemental de la sécurité de l'information, un état de situation démontrant sa conformité avec l'obligation prévue au paragraphe 1° ainsi que son respect des attentes en matière de sécurité de l'information, des orientations, standards, stratégies, directives, règles et

indications d’application pris en matière de sécurité de l’information en vertu de la Loi.

SECTION VII
ÉVÉNEMENTS DE SÉCURITÉ

16. Un organisme public doit tenir à jour un registre des événements de sécurité.

Ce registre doit comprendre notamment :

1° les coordonnées du chef de la sécurité de l’information organisationnelle (courriel, téléphone);

2° la date et l’heure de l’événement;

3° la localisation de l’événement (adresse);

4° la nature de l’événement;

5° la description de l’événement;

6° les préjudices engendrés et les personnes morales ou physiques concernées;

7° les actions prises;

8° l’acceptation ou non du risque résiduel et les justificatifs afférents;

9° les actions prévues;

10° la date de clôture de l’événement.

Sur demande du chef gouvernemental de la sécurité de l’information, une copie de ce registre doit lui être transmise dans le délai qu’il indique.

17. Si un événement de sécurité présente un risque qu’un préjudice sérieux soit causé, le chef de la sécurité de l’information organisationnelle doit, sans délai, en aviser le chef délégué de la sécurité de l’information auquel il est rattaché. À son tour, ce dernier avise, sans délai, le chef gouvernemental de la sécurité de l’information pour lui dresser l’état de situation.

Le présent article s’applique avec les adaptations nécessaires lorsqu’un chef délégué de la sécurité de l’information est également chef de la sécurité l’information organisationnelle en application du deuxième alinéa de l’article 10.

SECTION VIII
DISPOSITIONS DIVERSES ET FINALES

18. Le chef gouvernemental de la sécurité de l’information doit, au plus tard le 8 décembre 2026 et par la suite, tous les cinq ans, faire au Conseil du trésor un rapport sur l’application de la présente directive et sur l’opportunité de maintenir ou de modifier ses dispositions.

19. La présente directive remplace la Directive sur la sécurité de l’information gouvernementale prise par le Conseil du trésor le 10 décembre 2013 et approuvée par le décret numéro 7-2014 du 15 janvier 2014.

20. La présente directive entre en vigueur le 8 décembre 2021.

Secrétariat
du Conseil du trésor
Québec