Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale

23 novembre 1999

Gouvernement du Québec
Conseil du trésor
Sous-secrétariat aux inforoutes et aux ressources informationnelles

TABLE DES MATIÈRES

TABLE DES MATIÈRES **2**

SECTION I : DISPOSITIONS GÉNÉRALES **3**

§ 1 - OBJET DE LA DIRECTIVE 3
§ 2 - CHAMP D'APPLICATION 3
§ 3 - DÉFINITIONS 3

SECTION II : GESTION GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE ET DES ÉCHANGES ÉLECTRONIQUES **4**

§ 1 - PRINCIPES DIRECTEURS 4
§ 2 - RESPONSABILITÉS PARTICULIÈRES EN MATIÈRE DE GESTION GOUVERNEMENTALE DE LA SÉCURITÉ 5
Le Conseil du trésor et son secrétariat *5*
Le ministère de la Justice du Québec *6*
Le ministère des Relations avec les citoyens et de l'Immigration *6*
Le Conservateur des archives nationales du Québec *7*
Le Contrôleur des finances *7*
La Sûreté du Québec *7*
§ 3 – LES MINISTÈRES ET ORGANISMES *7*
Le responsable de la sécurité de l'information numérique *8*
§ 4 - LES INFRASTRUCTURES COMMUNES 9
Description générale *9*
Obligations des parties *9*

SECTION III : DISPOSITIONS FINALES **10**

SECTION I : DISPOSITIONS GÉNÉRALES

§ 1 - Objet de la directive

1. Cette directive énonce les principes directeurs en matière de sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, identifie les intervenants concernés par la gestion de cette sécurité, détermine les responsabilités des ministères et organismes et prévoit l'instauration des mécanismes de coordination et de collaboration appropriés en vue d'assurer la disponibilité, l'intégrité, la confidentialité de l'information numérique, l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent.

§ 2 - Champ d'application

2. Cette directive s'applique aux ministères et aux organismes dont le budget de fonctionnement est voté, en totalité ou en partie, par l'Assemblée nationale ou dont le personnel est nommé et rémunéré suivant la Loi sur la fonction publique (chapitre F-3.1.1).

   Cette directive s'applique également à tout autre organisme public qui adhère à une infrastructure commune du gouvernement du Québec.

§ 3 - Définitions

3. Dans la présente directive, on entend par :

   a) ***cycle de vie de l'information numérique*** *:* la période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information ;

   b) ***infrastructure commune*** : l'ensemble des composantes matérielles, logicielles, technologiques et organisationnelles ainsi que les services communs y compris l'expertise technique utilisés en tout ou en partie par plusieurs ministères et organismes ;

   c) ***technologie de l'information*** : tout logiciel, matériel électronique ou combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, reproduire, protéger ou éliminer de l'information numérique ;

   d) ***Information numérique :*** information dont l'usage n'est possible qu'au moyen des technologies de l'information.

SECTION II : GESTION GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE ET DES ÉCHANGES ÉLECTRONIQUES

§ 1 - Principes directeurs

4. La sécurité contribue à la réalisation de la mission de l'État en protégeant sa renommée et la confiance des citoyens à l'égard des services publics. Elle prend tout son sens dans la poursuite des finalités de l'organisation dans le respect des obligations légales et administratives.

   Les ministères et organismes, qui sont les premiers responsables d'assurer la sécurité de l'information numérique qu'ils détiennent ou utilisent ainsi que celle des échanges électroniques, doivent mettre en œuvre un ensemble de mesures destinées à gérer les risques et leurs impacts à l'égard de :

   a) la « **disponibilité** », laquelle est la propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée ;

   b) l'« **intégrité »**, laquelle est la propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation ;

   c) la « **confidentialité** », laquelle est la propriété d'une information de n'être accessible qu'aux personnes autorisées ;

   d) l'« **authentification** », laquelle est un acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif ;

   e) l'« **irrévocabilité** », laquelle est la propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

5. Le sous-ministre ou le dirigeant d'organisme doit assurer la gestion de la sécurité conformément aux principes suivants :

   a) vision commune : l'atteinte d'un niveau de sécurité adéquat nécessite l'adhésion à une vision et une compréhension communes de la sécurité tant au sein des ministères et organismes que dans l'Administration gouvernementale ;

   b) cohérence : la sécurité repose sur une approche globale et intégrée qui tient compte des aspects humains, organisationnels, physiques, techniques et juridiques et demande la mise en place d'un ensemble de mesures coordonnées de prévention, de détection, de correction et de sanction ;

c) ***responsabilité et imputabilité*** : l'efficacité de la sécurité exige l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place de mécanismes de coordination et de contrôle permettant une reddition de comptes adéquate ;

d) ***évolution*** : les pratiques et solutions techniques retenues en matière de sécurité doivent être réévaluées périodiquement afin de tenir compte des changements organisationnels et technologiques ainsi que de l'évolution des menaces et des risques ;

e) ***universalité*** : les pratiques et solutions techniques retenues en matière de sécurité correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

§ 2 - Responsabilités particulières en matière de gestion gouvernementale de la sécurité

6. Le Conseil du trésor et son secrétariat, le ministère de la Justice du Québec, le ministère des Relations avec les citoyens et de l'Immigration, le Conservateur des archives nationales du Québec, le Contrôleur des finances et la Sûreté du Québec ont des responsabilités particulières dans la gestion coordonnée de la sécurité gouvernementale.

Le Conseil du trésor et son secrétariat

7. Le Conseil du trésor assure le rôle de gouverne de la sécurité. À cette fin, il détermine :

   a) les objectifs et les contrôles stratégiques à appliquer en matière de sécurité incluant les éléments de reddition de comptes requis ;

   b) les normes de sécurité ;

   c) les éléments obligatoires en matière de sécurité que doivent comporter les ententes et contrats conclus par les ministères et les organismes avec les fournisseurs de services, partenaires, mandataires et, sous réserve des exigences de la loi en matière d'ententes internationales et intergouvernementales, avec d'autres gouvernements ;

   d) les infrastructures communes de sécurité à mettre en place dans l'Administration gouvernementale, leurs composantes et les procédures et règles de gestion associées ainsi que les cas où leur utilisation est obligatoire en tout ou en partie ;

   e) un plan gouvernemental de sécurité prenant en compte les risques stratégiques et définissant les résultats à atteindre.

8. Le Secrétariat du Conseil du trésor coordonne l'application de la sécurité. À cette fin, il :

   a) propose au Conseil du trésor les objectifs et les contrôles stratégiques, les normes, les éléments obligatoires des ententes et contrats en matière de sécurité, les infrastructures communes, leurs composantes, les cas où leur utilisation est obligatoire et les procédures et règles de gestion associées ainsi que le plan gouvernemental de sécurité ;

   b) établit et diffuse les pratiques et outils requis pour supporter l'application des exigences de sécurité ;

   c) produit annuellement au Conseil du trésor, un état de situation gouvernemental de la sécurité portant notamment sur la réalisation du plan gouvernemental de sécurité ;

   d) voit à la mise en œuvre d'un programme gouvernemental de sensibilisation et de formation sur la sécurité de l'information numérique et des échanges électroniques ;

   e) instaure des mécanismes de coordination et de collaboration portant sur tous les aspects de la sécurité et favorise les projets de partenariat en la matière au sein de l'Administration gouvernementale ;

   f) instaure et coordonne un réseau d'experts et de vigie à l'échelle gouvernementale ayant comme but principal d'améliorer la sécurité en suivant l'évolution des menaces, des vulnérabilités et des solutions de sécurité.

Le ministère de la Justice du Québec

9. Le ministère de la Justice est chargé d'élaborer le cadre légal nécessaire pour assurer la sécurité juridique de la documentation et de l'information, ainsi que la valeur juridique des communications et des transactions effectuées au moyen des technologies de l'information, y compris celles de l'Administration gouvernementale. Il assure également un rôle conseil sur les questions de droit reliées à la sécurité de l'information numérique et des échanges électroniques auprès du Secrétariat du Conseil du trésor et des ministères et organismes afin que l'élaboration des critères juridiques, outils, guides, normes, clauses contractuelles ou tout autre document relatif à la sécurité soit conforme aux exigences de la loi et des règlements en cette matière.

Le ministère des Relations avec les citoyens et de l'Immigration

10. Le ministère des Relations avec les citoyens et de l'Immigration assure une fonction conseil de niveau gouvernemental en matière d'accès aux documents et de protection des renseignements personnels auprès du Secrétariat du Conseil du trésor et des ministères et organismes afin que les règles pertinentes soient intégrées dans l'élaboration des outils, guides, normes, séances de sensibilisation ou dans tout autre document relatif à la sécurité.

Le Conservateur des archives nationales du Québec

11. Le Conservateur des archives nationales du Québec contribue à l'établissement des normes et des exigences de sécurité en ce qui concerne la protection et la conservation de l'information ayant une valeur patrimoniale ou archivistique.

Le Contrôleur des finances

12. Le Contrôleur des finances conseille les ministères et organismes budgétaires dans l'élaboration et la mise en place des mesures de sécurité, lors du développement, de modifications importantes ou de refontes majeures des systèmes d'information à caractère financier. Il informe le Secrétariat du Conseil du trésor, par un rapport annuel, des résultats de ses travaux et des irrégularités qu'il juge utile de porter à son attention.

La Sûreté du Québec

13. La Sûreté du Québec assure auprès du secrétariat du Conseil du trésor un rôle conseil et une aide technique en matière d'évaluation des menaces et des risques stratégiques ainsi que dans les enquêtes touchant les délits informatiques.

§ 3 – Les ministères et organismes

14. Les ministères et organismes étant les premiers responsables de la sécurité des informations qu'ils détiennent ou utilisent pour leur propre compte ou celui d'un tiers, le sous-ministre ou le dirigeant d'organisme doit s'assurer du respect des lois, ainsi que des objectifs, directives et normes de sécurité déterminés par le Conseil du trésor et voir à ce que soit gérée la sécurité de l'information numérique et des échanges électroniques :

    a) dès la conception, la réalisation ou la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques ;

    b) durant tout le cycle de vie de l'information numérique.

15. Le sous-ministre ou le dirigeant d'organisme doit, en matière de sécurité :

    a) définir clairement les valeurs organisationnelles et les orientations internes, les faire partager par l'ensemble de son personnel et les communiquer à ses partenaires pour s'assurer qu'elles sont respectées ;

    b) instaurer un mécanisme d'identification et d'évaluation périodique des risques ainsi que de l'adéquation des mesures de sécurité en vigueur par rapport à ces derniers ;

c) établir un plan global de sécurité, incluant les mesures de sécurité à mettre en œuvre, et le réviser périodiquement ;

d) assigner la responsabilité de toute information numérique ou technologie de l'information à un détenteur qui devra s'assurer en collaboration avec le responsable de la sécurité de l'information numérique que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement ; de plus, le nom des détenteurs et leurs responsabilités devront être consignés dans un registre d'autorité de la sécurité ;

e) intégrer aux ententes et aux contrats des dispositions garantissant le respect des exigences de sécurité comportant les éléments obligatoires déterminés par le Conseil du trésor ;

f) faire en sorte que le niveau de sécurité appliqué aux informations numériques qu'il reçoit ou communique à un autre ministère ou organisme ou à un tiers rencontre les exigences prescrites par la loi, les règlements ou les directives ;

g) assurer la sensibilisation et la formation de son personnel en matière de sécurité ;

h) procéder à l'analyse formelle et systématique des événements ayant mis ou qui auraient pu mettre en péril la sécurité ;

i) mettre en place des mécanismes d'évaluation et de contrôle assurant l'application et l'efficacité des orientations et mesures de sécurité retenues impliquant notamment les vérificateurs internes ;

j) produire annuellement au secrétariat du Conseil du trésor les bilans et états de situation conformément aux instructions de celui-ci ;

k) instaurer des mécanismes de coordination et de collaboration;

l) collaborer aux travaux du réseau d'experts et de vigie à la demande du Secrétariat du Conseil du trésor.

Le responsable de la sécurité de l'information numérique

16. Le sous-ministre ou le dirigeant d'organisme nomme un responsable de la sécurité de l'information numérique pour assurer la gestion et la coordination de la sécurité et le représenter en cette matière dans l'organisation.

Plus particulièrement, le responsable de la sécurité de l'information numérique :

a) soutient le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention ;

b) participe aux mécanismes de coordination et de collaboration et peut y représenter le sous-ministre ou le dirigeant d'organisme ;

c) s'assure de l'identification et de la gestion des risques d'atteinte à la sécurité ;

d) conçoit, propose pour approbation, met en œuvre et évalue un plan de sécurité permettant de réduire les risques à un niveau jugé acceptable par l'organisation ;

e) identifie les risques résiduels que doit assumer le sous-ministre ou le dirigeant d'organisme ;

f) s'assure de la prise en compte des orientations et exigences en matière de sécurité lors de la conception, de la réalisation ou de la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques et donne un avis de pertinence aux gestionnaires et aux détenteurs concernés ;

g) élabore et tient à jour le registre d'autorité de la sécurité.

§ 4 - Les infrastructures communes

Description générale

17. Une infrastructure commune de sécurité déterminée par le Conseil du trésor est fournie par le secrétariat du Conseil du trésor (Services gouvernementaux). Cependant, le Conseil du trésor peut mandater tout autre ministère ou organisme pour qu'il fournisse une infrastructure commune.

Obligations des parties

18. Le sous-ministre ou le dirigeant d'organisme qui adhère à une infrastructure commune et le fournisseur d'infrastructure doivent conclure une entente. Cette entente prévoit notamment des exigences de sécurité, un niveau de service et des procédures opérationnelles coordonnés.

19. Le ministère ou l'organisme responsable de fournir les infrastructures communes doit produire annuellement, conformément aux instructions reçues du Secrétaire du Conseil du trésor, un état de situation de la sécurité de cette infrastructure commune qui sera intégré à son bilan annuel de la sécurité.

SECTION III : DISPOSITIONS FINALES

20. Le Secrétariat du Conseil du trésor, de concert avec les ministères et les organismes, devra présenter au Conseil du trésor une évaluation de l'application de cette directive au plus tard trois années après son adoption.

21. La présente directive remplace la Directive concernant la sécurité de l'information électronique et des actifs informationnels adoptée par la décision du Conseil du trésor du 20 avril 1993 (C.T. 182895).

22. La présente directive entre en vigueur le 23 novembre 1999 et prend effet le 4 février 2000.