Ministère
du Développement durable,
de l'Environnement
et de la Lutte contre les
changements climatiques
Québec

Bureau des renseignements, de l'accès à l'information
et des plaintes sur la qualité des services

PAR COURRIEL

Le 20 octobre 2015

Objet : Demande d'accès # 2015-07-39 – Lettre réponse

Madame,

Nous donnons suite à votre demande, reçue le 10 juillet 2015, concernant tout document relatif aux activités de formation et de sensibilisation du personnel du ministère du Développement durable, de l'Environnement et de la Lutte contre les changements climatiques en matière de protection des renseignements personnels pour les années 2014 et 2015.

Vous trouverez en annexes les documents demandés. Il s'agit de :

1. Formation, 13 janvier 2013, 1 page;
2. Campagne de sensibilisation 2013, 13 janvier 2013, 1 page;
3. Sécurité de l'information, 13 janvier 2015, 1 page;
4. Documentation, 24 mars 2015,1 page;
5. Politique ministérielle de sécurité de l'information, novembre 2008, 9 pages;
6. Directive ministérielle sur la sécurité de l'information numérique et des échanges électroniques, novembre 2009, 28 pages;
7. Directive ministérielle de sécurité liée à l'utilisation des terminaux sans fil, décembre 2011, 8 pages;
8. Introduction à la sécurité de l'information, 13 janvier 2015, 4 pages.

Conformément à l'article 51 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1), nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information. Vous trouverez en pièce jointe une note explicative concernant l'exercice de ce recours.

Si vous désirez des renseignements supplémentaires, vous pouvez vous adresser à M^me^ Alexie Gauthier, analyste de votre dossier, à l'adresse courriel : alexie.gauthier@mddelcc.gouv.qc.ca en mentionnant le numéro du dossier en objet.

Veuillez agréer, Madame, l'expression de nos sentiments les meilleurs.

Le Bureau d'accès à l'information,

ORIGINAL SIGNÉ PAR

Julie Bissonnette

p. j. (9)

Édifice Marie-Guyart, 29e étage
675, boul. René-Lévesque Est, boîte 13
Québec (Québec) G1R 5V7
Téléphone : 418 521-3858
Télécopieur : 418 643-0083
Courriel : acces@mddelcc.gouv.qc.ca
Internet : www.mddelcc.gouv.qc.ca

Développement durable, Environnement et Lutte contre les changements climatiques
Québec

Formation

La campagne de sensibilisation à la sécurité de l'information s'articule autour d'une plateforme de cours en ligne. Celle-ci comporte quatre modules à compléter selon un parcours trimestriel (3 mois pour chaque module). Chaque module comporte des trucs et conseils et propose de cours exercices que vous pouvez effectuer en quelques minutes, selon vos disponibilités.

Voici les sujets dont vous traiterez au cours de votre cheminement :

Premier trimestre - Introduction à la sécurité de l'information

- La gestion des menaces et des risques
- La propriété intellectuelle
- La création d'un mot de passe efficace
- Le courrier électronique
- Les pourriels
- Les codes malicieux

Deuxième trimestre - La protection physique

- La protection physique
- Le principe du bureau propre
- Le contrôle d'accès
- L'ingénierie sociale
- « Bring your own device »

Troisième trimestre - La protection des informations sensibles

- La classification de l'information
- La gestion de l'information
- Les communications externes
- La protection des renseignements personnels
- La protection des cartes de crédit
- La destruction des renseignements et des actifs sensibles
- Le vol d'identité

Quatrième trimestre - L'internet et le travail à distance

- La confidentialité sur le Web
- Le bon usage d'Internet au travail
- Les réseaux sociaux
- Les utilisateurs nomades
- La sécurité des téléphones intelligents
- La sécurité dans les nuages (Cloud computing)

Testez vos connaissances

Accéder à la plate-forme de formation en ligne :

Retour à l'index

Mise à jour : 2015-01-13

Source : Lucie Racine
Direction générale des technologies de l'information
418 521-3838, poste 4254

Développement durable, Environnement et Lutte contre les changements climatiques
Québec

Campagne de sensibilisation 2013

Cette campagne vise à sensibiliser et à responsabiliser davantage le personnel du Ministère.

La sécurité de l'information, ça se passe au quotidien, dans notre environnement de travail, et c'est à chacun de nous d'y voir.

Objectifs de la campagne

- Démontrer l'importance de protéger les renseignements confidentiels et stratégiques du Ministère
- Augmenter les connaissances du personnel en matière de sécurité de l'information, particulièrement en ce qui a trait aux comportements à risques et aux bonnes pratiques à adopter.
- Outiller les employés afin d'orienter leurs gestes et de faciliter leur prise de décisions
- Développer une préoccupation durable en intégrant la sécurité de l'information au quotidien

Quelle est l'attente du Ministère envers vous?

Le Ministère a la responsabilité d'assurer la sécurité de l'information qu'il détient, qu'il traite et d'utiliser les technologies de l'information dans le respect des règles.

Le Ministère attend donc de son personnel qu'il agisse de façon responsable en respectant les politiques et directives en vigueur, en adoptant les bonnes pratiques et en appliquant les mesures de sécurité recommandées au Ministère.

Soyez vigilants dans la gestion de l'information que vous recueillez, consultez, traitez ou communiquez!

Testez vos connaissances

Accéder à la plate-forme de formation en ligne :

Retour à l'index

Mise à jour : 2015-01-13

Source : Lucie Racine
Direction générale des technologies de l'information
418 521-3838, poste 4254

Développement durable, Environnement et Lutte contre les changements climatiques
Québec

Sécurité de l'information

Campagne de sensibilisation 2013
Thématique et objectifs de la campagne

Introduction à la sécurité de l'information
Notions de bases en sécurité de l'information - Initiation aux principes de la sécurité de l'information numérique et des technologies de l'information - Aide mémoire

Documentation
Documentation ministérielle et gouvernementale en matière de sécurité de l'information (politiques, directives, guides)

Formation
Informations sur les cours en ligne

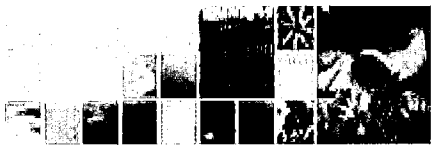
C'est mon affaire : c'est s0r!

Mise à jour : 2015-01-13

Source : Lucie Racine
Direction générale des technologies de l'information
418 521-3838, poste 4254

Québec

Développement durable, Environnement et Lutte contre les changements climatiques
Québec



Documentation

Politique ministérielle de sécurité de l'information

Cette politique a pour objet d'assurer la sécurité de l'information qui est sous la responsabilité du ministère du Développement durable, de l'Environnement et des Parcs, quel que soit le support de cette information (numérique, papier ou autres) et sa localisation. Également, elle établir les rôles et responsabilités de chacun.

Directive ministérielle sur la sécurité de l'information numérique et des échanges électroniques

Cette directive établit les orientation et les règles relatives à l'utilisation des services des réseaux électroniques du Ministère afin d'assurer l'intégrité des systèmes, la protection des renseignements personnels et la sécurité des échanges électroniques d'information.

Directive ministérielle de sécurité liée à l'utilisation des terminaux sans fils

Cette directive établit les orientations et les règles relatives à l'utilisation des terminaux sans fil au Ministère. Inclut les assistants numériques personnels (BlackBerry, Palm et autres), téléphones cellulaires et ordinateurs portables.

Autres références

Pour toute information sur d'autres références gouvernementales en matière de sécurité de l'information, consultez la section Sécurité informatique.

Actifs informationnels

Le personnel du Ministère, doit être conscient de l'importance pour l'organisation des mesures de protection de l'information en vigueur afin d'assurer la sécurité de l'information.

La sécurité de l'information couvre et vise à protéger l'ensemble des actifs informationnels utilisés par l'organisation dans la conduite des ses activités.

Dans le domaine de la sécurité de l'information, sont considérés comme étant des actifs informationnels, les éléments suivants :

- Un employé
- Un immeuble

- Une donnée (fichier, dossier, etc.)
- Un service
- Un système informatique
- De l'équipement supportant une donnée
- Les systèmes de télécommunications

Procédures / Bonnes pratiques

- Procédure de gestion des incidents de sécurité informatique
- Procédure ministérielle lors du départ d'une personne
- Procédure d'accès au local de formation du 3e étage
- Mesures pour assurer la sécurité physique des équipements
- Engagement de confidentialité
- Processus de vérification d'un poste de travail en cas de contravention aux règles de sécurité, voir la section 20 de la directive, p. 24
- Pratiques recommandées pour accroître la sécurité des ordinateurs portatifs
- Procédure relative au burinage des équipements
- Utilisation des espaces de stokage

Protection de l'accès au poste de travail

- Confidentialité de l'identifiant et du mot de passe, voir la section 6.1 de la directive, p. 13

Retour à l'index

Mise à jour : 2015-03-24

Source : **Lucie Racine**
Direction générale des technologies de l'information
418 521-3838, poste 4254

Québec

Développement durable,
Environnement
et Parcs
Québec

Politique ministérielle de sécurité de l'information

Ministère du Développement durable, de l'Environnement et des Parcs

Novembre 2008

TABLE DES MATIÈRES

1. INTRODUCTION

En avril 2006, le Secrétariat du Conseil du trésor adopte la *Directive sur la sécurité de l'information gouvernementale* (C.T. 203560) qui remplace la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* (C.T. 194055) du 23 novembre 1999.

Cette directive, en vigueur depuis le 1er mai 2006, s'applique aux ministères et organismes visés par l'article 64 de la *Loi sur l'administration publique.*

Découlant de cette nouvelle directive, le Ministère a élaboré une « Politique ministérielle sur la sécurité de l'information » dans le respect de la législation applicable en la matière, dont une liste non exhaustive est présentée à l'annexe 1. Celle-ci remplace la politique ministérielle actuelle sur la sécurité de l'information numérique et des échanges électroniques.

2. LE CHAMP D'APPLICATION DE LA POLITIQUE

La politique ministérielle s'applique à l'information détenue ou utilisée par l'ensemble des unités administratives du MDDEP, et ce, tout au long de son cycle de vie et sans égard à sa localisation.

Plus particulièrement, cette politique interpelle le personnel du Ministère qui a accès à de l'information, de nature confidentielle, personnelle, stratégique ou autre et ce, sans égard au statut d'emploi. De plus, toutes les activités impliquant la manipulation ou l'utilisation de cette information, sous quelque forme que ce soit, qu'elles soient effectuées dans ses locaux, dans un autre lieu ou à distance sont assujetties à cette politique. En outre, elle doit être respectée à toutes les étapes de vie d'une information du début de sa réalisation à sa disposition finale.

3. L'OBJET DE LA POLITIQUE

La présente politique a pour objet d'assurer la sécurité de l'information qui est sous la responsabilité du ministère du Développement durable, de l'Environnement et des Parcs, quel que soit le support de cette information (numérique, papier ou autres) et sa localisation.

Elle veut aussi garantir la sécurité des moyens qui sont utilisés durant tout le cycle de vie de l'information comme :

- les supports des documents;
- les outils pour communiquer l'information, la consulter, la transmettre ou la conserver, qu'il s'agisse de systèmes informatiques, de canaux et moyens de communication, de réseaux de communication ou de transmission, ou d'autres moyens technologiques;
- les endroits, les installations, les objets ou les lieux où se trouve l'information;
- l'utilisation sur place ou à distance d'une information ou d'une ressource.

La présente politique a aussi pour objet d'établir les rôles et les responsabilités des ressources humaines chargées de la sécurité de l'information, dans ses aspects physiques, opérationnels ou de gestion documentaire.

4. ÉNONCÉS GÉNÉRAUX

La Politique sur la sécurité de l'information du Ministère est fondée sur les énoncés généraux suivants, lesquels constituent le fondement des règles, procédures et autres mesures de sécurité nécessaires à l'atteinte de ses objectifs :

- le Ministère adhère au cadre gouvernemental en matière de sécurité de l'information;
- les informations du Ministère sont essentielles à ses opérations courantes et font l'objet d'une utilisation et d'une protection adéquates;
- les informations de nature confidentielle, personnelle, stratégique, ou autre sont protégées contre tout accès ou toute utilisation non autorisé ou illicite;
- le Ministère s'engage à sensibiliser les personnes assujetties à la présente politique, ses fournisseurs et ses partenaires, de manière à susciter leur engagement et leur adhésion à une vision et une compréhension communes de la sécurité ;
- toute information est assignée à un détenteur qui est responsable de sa gestion et de l'application des mesures de contrôle nécessaires;
- chaque utilisateur participe à la protection de l'information mise à sa disposition et l'utilise avec discernement et aux seules fins prévues par le Ministère;
- toute information est dédiée et réservée uniquement à la réalisation de la mission du Ministère et des activités de gestion, de service et de recherche qui en découlent;
- l'information demeure, en tout temps, l'entière propriété du Ministère;
- le Ministère est en mesure de localiser l'information durant tout son cycle de vie;
- le Ministère assure la protection de la propriété intellectuelle et des droits d'auteurs;
- le citoyen ou le représentant de l'entreprise ou du partenaire du Ministère a le droit de s'informer de l'usage qui pourrait être fait des informations de nature confidentielle, personnelle, stratégique, ou autre qu'il fournit, et des catégories de personnes qui auront accès à ces informations;
- les ententes et les contrats contiennent des dispositions garantissant le respect des exigences en matière de protection et de sécurité de l'information;
- le Ministère dispose d'un processus de gestion des incidents de sécurité, afin d'en réduire les conséquences directes et indirectes;
- le Ministère met en œuvre un ensemble de mesures de protection et de sécurité destinées à assurer :

  La disponibilité

  Le Ministère assure la disponibilité en temps voulu et de la manière requise par les personnes autorisées :

  - en se dotant d'un processus adéquat permettant de retrouver facilement l'information, et dont le fonctionnement est vérifié en fonction des objectifs de l'organisation;
  - en consacrant des investissements aux mécanismes appropriés assurant la mise en place d'outils de surveillance régulière de la disponibilité de l'information ;
  - en s'engageant à rendre disponible de l'information ministérielle, en fonction d'appuyer l'offre de service du Ministère.

Intégrité

Pour assurer l'intégrité des documents qui la requièrent, notamment les documents essentiels à ses opérations courantes, le Ministère se dote des moyens permettant de vérifier que, durant tout leur cycle de vie, l'information de ces documents n'a pas été altérée, qu'elle est maintenue dans son intégralité et que le support qui la porte lui procure la stabilité et la pérennité voulues. Il s'assure :

- de contrôler que les informations qui entrent dans le réseau ministériel proviennent de sources connues, identifiables et vérifiables;
- d'évaluer régulièrement le fonctionnement des solutions mises en place en matière de sécurité de l'information (audits et autres);
- de consigner, dans des registres exploitables, les incidents relatifs à la sécurité de l'information, les analyser et en assurer le suivi à intervalles réguliers;
- de mettre en place des mécanismes permettant de vérifier l'intégrité de l'information.

Confidentialité

Pour protéger les renseignements personnels et pour préserver la confidentialité de l'information, le Ministère prend plusieurs mesures :

- il ne collige et ne conserve que l'information nécessaire à l'accomplissement de sa mission, dans le respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1);
- l'accès aux informations de nature confidentielle, personnelle, stratégique ou autre détenues par le Ministère doit être protégé;
- la destruction des documents dont l'information est devenue désuète ou inutile est effectuée conformément à la *Loi sur les archives* (L.R.Q., c. A-21.1) et selon les règles gouvernementales établies ;
- des mesures sont prises pour contrer l'usurpation d'identité et pour prévenir toute autre forme d'appropriation et d'utilisation frauduleuse, malveillante ou inadéquate de l'information, par des personnes ou des dispositifs situés à l'intérieur ou à l'extérieur du Ministère. Elles sont coordonnées avec les mesures de détection, de correction et de sanction appropriées ;
- l'accès aux locaux fait l'objet de mesures de sécurité appropriées.
- l'accès aux classeurs/filières contenant de l'information de nature confidentielle, personnelle, stratégique ou autre doit faire l'objet de mesures de sécurité appropriées.

5. LES PRINCIPES DIRECTEURS

La sécurité de l'information permet de maintenir et de rehausser la confiance de la clientèle à l'égard des services que le MDDEP rend. Elle contribue à la réalisation de sa mission et vise également à assurer la pérennité d'une information fiable.

Le MDDEP assure la sécurité de ses informations conformément aux principes directeurs suivants :

- la protection : les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger. Elles sont établies en fonction des risques et impacts s'y rattachant et en tenant compte de la sensibilité et de la finalité de l'information ;

- la responsabilité et l'obligation de rendre compte : l'efficacité de la sécurité de l'information exige l'attribution claire de responsabilités à tous les niveaux du MDDEP (notamment avec ses partenaires, fournisseurs et clientèles respectives), ce qui permet une reddition de comptes adéquate ;
- l'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, humains et technologiques, ainsi que de l'évolution des menaces et des risques ;
- l'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 ou au sein de l'appareil gouvernemental québécois ;
- l'éthique : le processus de gestion de la sécurité de l'information doit être soutenu par une prise en charge des enjeux d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle, conformément aux règles d'éthique de la fonction publique. Cette approche vise à assurer l'intégrité, la transparence et l'efficacité du MDDEP en toute circonstance.

6. MISE EN ŒUVRE DE LA SÉCURITÉ DE L'INFORMATION

La sécurité de l'information repose sur la gestion intégrée de l'ensemble de l'information et sur une approche qui tient compte des dimensions éthiques, juridiques, humaines, organisationnelles et techniques. Elle suppose la prise de mesures de sécurité physique, logique et opérationnelle ainsi que des mesures de gestion documentaire.

Ces mesures de sécurité sont envisagées dès la création de l'information jusqu'à sa disposition finale. Elles couvrent notamment les processus, les procédures, les applications, les infrastructures ainsi que les moyens et les supports utilisés pour consulter, traiter, transmettre et conserver l'information.

Tout au long du cycle de vie de l'information, la sécurité est une priorité. Elle nécessite la mise en place d'actions coordonnées de prévention, de détection, de correction et de sanction.

7. RÔLES ET RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

En matière de sécurité de l'information, le Ministère a élaboré une structure de gouvernance qui précise les rôles et responsabilités de l'ensemble des acteurs impliqués en ce domaine. Le document est disponible sur l'intranet ministériel à l'adresse suivante : http://intranet/outils/techno/securite-informatique/index.htm

Parmi les acteurs principaux mentionnons :

La sous-ministre s'assure du respect des lois ainsi que des objectifs, directives et normes de sécurité déterminés par le Conseil du trésor et voit à ce que soit gérée et coordonnée la sécurité de l'information.

Nommé par la sous-ministre, le responsable de la sécurité de l'information (RSI) assure la gestion et la coordination de la sécurité et la représente en cette matière.

La responsable de l'accès aux documents et de la protection des renseignements personnels participe aux mécanismes de coordination et de concertation en sécurité de l'information.

Le responsable de la gestion documentaire s'assure de la prise en compte des orientations et exigences en matière de sécurité en gestion des documents et donne un avis de pertinence aux gestionnaires et aux détenteurs concernés.

Les gestionnaires des unités administratives sont responsables de la sécurité de l'information relevant de leur secteur respectif. Ils mettent en place des mesures de contrôle appropriées.

L'utilisateur (incluant les mandataires, partenaires et fournisseurs du Ministère) a la responsabilité de protéger l'information mise à sa disposition et de l'utiliser avec discernement.

8. MESURES ADMINISTRATIVES ET SANCTIONS

Conformément au plan ministériel de délégation des pouvoirs en matière de gestion des ressources humaines et en collaboration avec la Direction des ressources humaines (DRH), le gestionnaire de l'unité administrative, détermine, selon la nature ou la gravité du cas, s'il est opportun d'appliquer une sanction disciplinaire ou de prendre une mesure administrative lorsqu'un membre de son personnel contrevient à cette Politique ou aux lignes directrices internes reliées à la sécurité de l'information.

9. DISPOSITIONS FINALES

9.1. Révision

La politique est révisée régulièrement afin de tenir compte des nouveaux besoins et de l'évolution des pratiques et des technologies.

9.2. Mise en application et suivi de la politique

Le responsable de la sécurité de l'information (RSI) est chargé de l'application de la présente politique.

10. APPROBATION ET ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son approbation par la sous-ministre.

Approuvée le : _____

La sous-ministre : _____
Madame Madeleine Paulin

Annexe 1

CADRE LÉGAL ET ADMINISTRATIF

La présente politique s'appuie principalement sur les lois et les directives suivantes:

- la *Charte canadienne des droits et libertés* (1982), L.R.C. (1985), App. II, no. 44;
- le *Code criminel*, L.R.C. 1985, c. C-46;
- la *Loi sur le droit d'auteur,* L.R.C. 1985, c. C-42;
- la *Charte des droits et libertés de la personne du Québec,* L.R.Q., c. C-12;
- le *Code civil du Québec,* C.c.Q.;
- la *Loi sur la sécurité civile*, L.R.Q., c. S-2.3;
- la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1;
- la *Loi sur les archives,* L.R.Q., c. A-21.1;
- la *Loi sur l'administration publique,* L.R.Q., c. A-6.01;
- la *Loi sur la fonction publique*, L.R.Q., c. F-3.1.1;
- le *Règlement sur l'éthique et la discipline dans la fonction publique,* L.R.Q., c. F-3.1.1, r.0.4;
- la *Directive sur la sécurité de l'information gouvernementale* (CT 203560 du 11 avril 2006);
- la *Directive sur l'utilisation éthique du courriel, d'un collecticiel, et des services d'Internet par le personnel de la fonction publique* (CT 198872 du 1er octobre 2002);
- la *Directive sur le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible* (CT 193953 du 19 octobre 1999 modifié par CT 199891 du 27 mai 2003);
- la *Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire* (CT 197658 du 13 février 2002 modifié par CT 198678 du 13 août 2002 et CT 200759 du 16 mars 2004);
- la *Politique ministérielle d'utilisation du courriel, du collecticiel et des services d'Internet*;
- la *Procédure ministérielle de traitement et de destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible.*

Ministère du
Développement durable,
de l'Environnement
et des Parcs
Québec

Directive ministérielle sur la sécurité de l'information numérique et des échanges électroniques

Comité ministériel de la sécurité de l'information

Québec, Mai 2006

(Mise à jour : Novembre 2009)

Rédaction de la version originale :

Comité ministériel de la sécurité de l'information

Robert Parent
Karl McKenna

Pour tout renseignement supplémentaire ou tout commentaire concernant cette Directive, vous êtes invités à communiquer auprès de :

Robert Parent
Coordonnateur de la sécurité de l'information numérique

Direction des ressources informationnelles
675, René Lévesque Est, 2e étage
Québec (Québec) GIR 5V7
Téléphone : 418 521-3838, poste 4254
Télécopieur : 418 643-8999
Courriel : robert.parent@mddep.gouv.qc.ca

Note : *Dans le présent document, le générique masculin n'est utilisé sans aucune discrimination et uniquement dans le but d'alléger le texte.*

Mise à jour : Novembre 2009 (Robert Parent)

TABLE DES MATIÈRES

Directive ministérielle sur la sécurité de l'information numérique et des échanges électroniques

1. Contexte

Cette Directive contient certaines règles de sécurité fondamentales en matière de travail et sur des valeurs qui se traduisent dans des comportements de respect à l'égard des services publics que nous rendons aux citoyennes et aux citoyens. Elle précise certaines obligations découlant de la « *Politique ministérielle de sécurité de l'information*».

2. Objectif

La présente Directive a pour objectif de :

- établir et faire connaître aux utilisateurs les orientations régissant l'utilisation des ressources informationnelles ;
- sensibiliser les utilisateurs aux risques associés à l'usage des technologies de l'information ;
- promouvoir les meilleurs intérêts du ministère, avec l'intention de fournir à chacun de ses employés tous les accès requis pour qu'il soit en mesure d'effectuer son travail ;
- fournir les conditions préalables à la mise en application des mesures de sécurité de l'information, qui sont essentielles à la réalisation de la mission du ministère, en vue d'assurer :
  - la disponibilité des ressources informationnelles ;
  - l'intégrité de l'information recueillie, emmagasinée et utilisée ;
  - la confidentialité de l'information sensible échangée et détenue ;
  - l'authentification des utilisateurs, de même que, lorsque requis, l'irrévocabilité des actions et des documents électroniques qui en découlent ;
  - la continuité des services informatiques, notamment par le rétablissement de ces services et la récupération des documents jugés essentiels, à la suite d'un sinistre ;
  - l'utilisation adéquate des services de l'inforoute ;
  - la gestion de la sécurité de l'information dès la conception, la réalisation ou la modification des systèmes d'information ou des infrastructures technologiques ;
  - le développement et le maintien d'un environnement sécuritaire et respectueux des droits collectifs et individuels ;
  - une gestion efficace de la sécurité de l'information ;

- l'amélioration de la sécurité en suivant l'évolution des menaces, des vulnérabilités et des solutions de sécurité ;
- la gestion des interventions lors d'un incident de sécurité.

3. Champ d'application

3.1 Personnes visées

Tout le personnel du ministère et toute personne ayant accès aux informations du ministère dans l'exécution de ses fonctions ou dans le cadre d'une prestation de travail ou de services effectuée pour le compte d'un partenaire ou d'un fournisseur, et qui utilise les ressources informationnelles du ministère dans ses locaux, à un autre endroit, ou à distance.

3.2 Actifs visés

Cette Directive s'applique à l'information et aux ressources informationnelles appartenant et détenues par le ministère. Elle s'applique donc aux équipements et applications informatiques ainsi qu'à la documentation nécessaire à leur bon fonctionnement, aux logiciels, aux traitements informatiques, aux données traitées par ordinateur ainsi qu'à tous les documents produits ou reçus dans le cadre des opérations numériques du ministère.

3.3 Activités visées

Toutes les activités impliquant le traitement de l'information ou l'utilisation sous toutes ses formes des ressources informationnelles du ministère sont visées par la présente, que celles-ci soient conduites dans ses locaux, à un autre endroit, ou à distance.

4. Énoncés généraux

La Directive sur la sécurité de l'information et des échanges électroniques du ministère est fondée sur les énoncés généraux suivants, lesquels constituent le fondement des règles, procédures et autres mesures de sécurité nécessaires à l'atteinte de ses objectifs :

- les ressources informationnelles du ministère sont essentielles à ses opérations courantes et font l'objet d'une utilisation et d'une protection adéquates ;
- les ressources informationnelles catégorisées confidentielles, les renseignements stratégiques, les renseignements industriels, financiers, commerciaux, scientifiques, techniques ou personnels sont protégées contre tout accès ou toute utilisation non autorisé ou illicite ; sont notamment confidentiels les renseignements nominatifs au sens de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* » *(http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html)* ;
- toute information emmagasinée ou consignée sur l'équipement électronique ministériel, est réputée constituer une information à laquelle le ministère a accès ;
- lorsqu'un employé emprunte une ressource, il prend les dispositions pour en assurer l'intégrité et la protection physique et logique;
- le ministère n'assume aucune responsabilité, directe ou indirecte, pour les pertes, dommages ou inconvénients causés aux utilisateurs à l'occasion ou en conséquence de l'utilisation des équipements et des ressources informationnelles, de télécommunication, ainsi que du réseau, ou advenant le cas où il devrait, pour quelque cause que ce soit, diminuer ses

services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions, ou encore arrêter définitivement ses services ;

- l'utilisateur est responsable des dommages qu'il peut causer par la diffusion sur le réseau d'informations non autorisées ou qui débordent l'exécution de ses fonctions. Il est également responsable des conséquences, réclamations ou dommages pouvant résulter de l'installation ou de l'usage d'un logiciel, progiciel ou programme non autorisé ou illégal.

5. Rôles et responsabilités

Il existe deux types de profils de responsabilités liés à la gestion de la sécurité de l'information et des échanges électroniques au ministère :

Les responsables de l'administration de la sécurité sont :

- la sous-ministre ;
- le comité ministériel de sécurité[1] de l'information ;
- le responsable de la sécurité de l'information (RSI) ;
- le détenteur de système ;
- le détenteur des services horizontaux ;
- le vérificateur interne du ministère.

Les responsables de l'utilisation sécuritaire des ressources informationnelles sont :

- le gestionnaire des utilisateurs d'une ressource informationnelle ;
- le responsable de la sécurité de l'information numérique (RSIN) ;
- le coordonnateur de la sécurité de l'information numérique ;
- l'utilisateur d'une ressource informationnelle ;
- les répondants désignés de la sécurité informatique ;
- le répondant désigné de la sécurité de la gestion documentaire ;
- le responsable de la sécurité matérielle ;

Les sections suivantes contiennent une brève description des rôles et responsabilités de chacun de ces intervenants à l'égard de la sécurité de l'information et des échanges électroniques.

5.1 Les responsables de l'administration de la sécurité

Les rôles et responsabilités des responsables de l'administration de la sécurité sont définis dans la « Politique ministérielle de sécurité de l'information ».

5.2 Les responsables de l'utilisation sécuritaire des ressources informationnelles

5.2.1 Le gestionnaire des utilisateurs d'une ressource informationnelle

- est un gestionnaire d'une unité administrative ;

[1] Dont la composition inclut le responsable de la sécurité de l'information ainsi que la personne responsable de la protection des renseignements personnels.

- se conforme aux directives de sécurité émises par le ministère et par les organismes du gouvernement du Québec ;
- assume la gestion de la sécurité de son unité administrative, en accord avec la présente Directive ;
- applique la « *Procédure à suivre par le gestionnaire lors du départ d'un employé* » (http://intranet/Organisation/directions/dgsgmt/dri/procedure/depart.pdf) ;
- autorise toute installation sur un poste de travail de son unité administrative de logiciels, de progiciels ou de programmes (réf. 8.1) ;
- autorise l'accès Internet à son personnel (réf. 13.2) ;
- informe son personnel du contenu de cette Directive et intervient en cas de manquement ;
- s'assure de la sensibilisation de tout nouvel employé, dès son entrée en fonction ;
- respecte le caractère confidentiel de l'information emmagasinée par son personnel lors de toute intervention de gestion ;
- prend des mesures adéquates afin que son personnel puisse travailler dans un environnement garantissant la sécurité et la confidentialité des informations ;
- gère les incidents de sécurité à effet localisé à son unité administrative ;
- autorise toute dérogation à la Directive sur la sécurité de l'information numérique et des échanges électroniques qui s'applique aux actifs dont il a la responsabilité (réf. 22.3);
- procède à une vérification de la sécurité s'il a des motifs raisonnables de croire qu'un employé contrevient à cette Directive (réf. 20.1) ;
- prévient son employé si son privilège d'accès est suspendu (réf. 20.2) ;
- impose des mesures administratives ou disciplinaires, conformément au plan ministériel de délégation des pouvoirs en matière de gestion des ressources humaines s'il y a lieu (réf. 21) ;
- informe le coordonnateur de la sécurité de l'information numérique de tout manquement à la présente Directive et collabore aux suites à donner ;
- désigne un représentant de la sécurité pour son unité administrative ayant pour mission de le seconder dans ses tâches et de le remplacer au besoin ; ce dernier se conforme aux normes et directives de la DRI dans l'exécution de ses tâches.

5.2.2 RSIN

Nommé par le RSI, celui-ci :

- remplace le RSI au besoin et le supporte dans ses tâches;
- préside le comité Directeur de tous les projets de sécurité;
- fait rapport au RSI et lui rend compte de l'état d'avancement des dossiers de sécurité de l'information numérique ;

5.2.3 Coordonnateur de la sécurité de l'information numérique

Le coordonnateur de la sécurité de l'information numérique, agit à titre de représentant désigné par le RSI, pour coordonner la sécurité de l'information numérique du ministère. À cet effet, il :

- propose les orientations de sécurité de l'information numérique et les communique au personnel et aux partenaires du ministère ;
- élabore et fait le suivi et la mise à jour périodique du plan global de la sécurité de l'information numérique ;
- assume la coordination des grands projets de sécurité ;
- fait rapport au RSI et lui rend compte de l'état d'avancement des dossiers de sécurité de l'information numérique ;
- veille à la conception, à l'application, à la mise à jour, à la coordination et à la vérification des normes et des procédures de sécurité de l'information numérique;
- coordonne la gestion opérationnelle de la sécurité notamment en élaborant des mesures de sécurité informatique, en proposant des dispositifs de sécurité et en dressant des plans de continuité;
- conserve un registre de toute dérogation à cette Directive signalée par les détenteurs;
- conserve un registre des incidents qui lui sont rapportés et en avise le Comité ministériel;
- supporte le RSI dans ses tâches.

5.2.4 L'utilisateur d'une ressource informationnelle

- respecte la présente Directive ;
- respecte les droits d'auteurs (réf. 8.3) ;
- participe à la protection des ressources informationnelles mises à sa disposition, en les utilisant avec discernement et aux seules fins prévues ;
- est responsable de la gestion sécuritaire de son code d'accès personnel (identifiant) et de son mot de passe (réf. 6.4) ;
- change son mot de passe régulièrement (réf. 6.4) ;
- assume la responsabilité de la protection de ses données et de l'accès à celles-ci ;
- assume la responsabilité de l'utilisation qu'il fait des ressources informationnelles du ministère ;
- assume la responsabilité de toutes les communications initiées par l'utilisation de son identifiant et de son mot de passe, et il voit à les protéger ;
- s'assure que le sauve-écran avec mot de passe est actif ou verrouille la session de travail avant de quitter son poste ;
- se choisit un mot de passe sécuritaire respectant les règles émises par la Direction des ressources informationnelles ;
- se préoccupe de préserver la réputation et la crédibilité du ministère.

Il lui est interdit de :

- tenter de déchiffrer, découvrir ou obtenir l'identifiant ou le mot de passe d'un autre utilisateur (réf. 6.4) ;
- noter son mot de passe sur un support papier ou électronique aisément accessible (réf. 6.4) ;
- consulter les données affichées ou disponibles à partir d'un poste de travail laissé sans surveillance par son utilisateur ;
- monopoliser ou abuser des ressources informationnelles (réf. 7.3) ;
- modifier ou détruire les logiciels, les progiciels, les programmes, les systèmes d'information, les équipements informatiques (réf. 7.8) ;
- désactiver l'antivirus de son poste de travail ou en changer la configuration (réf. 8.4) ;
- nuire volontairement au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, etc. ;
- utiliser des programmes, des logiciels ou autre moyens en vue d'intercepter, de collecter, de prendre connaissance, de déchiffrer ou de décoder de l'information véhiculée sur un réseau ou résidant sur un poste de travail.

5.2.5 Les répondants désignés de la sécurité informatique

Les répondants désignés de la sécurité informatique agissent à titre de représentants du détenteur des services horizontaux et des informations qu'ils supportent. C'est le directeur de la DRI, ou son représentant, qui les désigne.

5.2.6 Le répondant désigné de la sécurité de la gestion documentaire

Le répondant désigné de la sécurité de la gestion documentaire[2] effectue le suivi des changements et l'entretien des mesures ministérielles de sécurité documentaire contenues dans les outils de gestion documentaire (calendrier de conservation, procédures de gestion documentaire, etc.). Il conseille et assiste également les employés pour l'application de ces mesures de protection documentaire.

5.2.7 Le responsable de la sécurité matérielle

Le responsable de la sécurité matérielle[3] agit à titre de gestionnaire de la sécurité physique des lieux et des personnes. Il est responsable du contrôle d'accès physique aux immeubles du ministère.

6 Identifiant et mot de passe (identification et authentification)

6.1 Confidentialité de l'identifiant et du mot de passe

Les moyens d'accès ou d'identification (identifiant, mot de passe, carte magnétique, etc.) sont alloués à titre strictement **personnel et confidentiel et ne sont pas transférables**. Ces moyens d'accès sont révocables en tout temps. Les objets matériels servant à l'identification sont remis à la fin du lien d'emploi avec le ministère ou à la fin du contrat. Voir la « *Procédure à suivre par le gestionnaire lors du départ d'un employé* » (http://intranet/Organisation/directions/dgsgmt/dri/procedure/depart.pdf).

---

[2] Cette responsabilité relève du gestionnaire responsable de la gestion documentaire.
[3] Cette responsabilité relève de la Direction des ressources financières et matérielles.

6.2 Attribution et modification

Le code d'identification personnel est attribué en fonction des tâches que son titulaire accomplit dans le cadre de son travail. L'attribution d'un code d'identification ne donne pas de privilèges spéciaux, sauf si ce code est celui d'un administrateur.

Toute demande de création, modification ou destruction d'un code d'identification s'effectue en respectant le processus officiel du ministère, soit l'utilisation du formulaire « *Accès aux ressources informationnelles* »
(*http://srdri/SST/Formulaire_demande_identifiant_pr_secretaires_v4.htm*). Ce processus permet d'assurer l'autorisation, l'imputabilité et l'irrévocabilité de la demande.

6.3 Mécanisme technologique d'authentification

Un mécanisme technologique peut être ajouté à l'identifiant et au mot de passe, visant à augmenter le niveau d'authentification d'un utilisateur. Ce mécanisme est personnalisé pour chaque utilisateur. La gestion en est assurée par la Direction des ressources informationnelles.

6.4 Responsabilité de l'utilisateur

Chaque utilisateur du ministère est responsable de la gestion sécuritaire de son code d'accès personnel (identifiant) et particulièrement de son mot de passe. Un mot de passe n'est jamais divulgué, même pour une intervention de courte durée. Dans le cas où l'utilisateur a des raisons de croire et/ou soupçonne que son mot de passe personnel est connu d'un tiers, il le change immédiatement.

Le mot de passe est changé régulièrement et périodiquement, conformément aux modalités, critères et paramètres en vigueur sur le réseau ministériel. Voir la foire aux questions sur ce sujet au lien suivant : (http://intranet/Outils/techno/securite-informatique/questions.htm).

Afin de protéger le réseau informatique contre toute intrusion indésirable par usurpation d'identité, un utilisateur ne note jamais un mot de passe sur un support papier ou électronique aisément accessible, de même qu'il n'obtient ou ne tente d'obtenir tout mot de passe d'un autre utilisateur.

L'usurpation d'identité, c'est-à-dire l'utilisation d'un identifiant et d'un mot de passe de quelqu'un d'autre, est une offense au code criminel.

6.5 Codes d'identification d'administrateurs

La création d'un code d'identification d'administrateur permet en tout temps d'identifier son utilisateur et de retracer ses interventions, à la suite d'un incident.

Le code d'identification d'administrateur ne sert qu'aux fins administratives pour lesquelles il a été créé. Toute autre opération est effectuée avec le code d'identification personnel.

6.6 Suspension et suppression de l'identifiant

La suspension du code d'identification d'un utilisateur s'effectue dès le départ de cette personne du ministère en conformité avec la « *Procédure à suivre par le gestionnaire lors du départ d'un employé* » (http://intranet/Organisation/directions/dgsgmt/dri/procedure/depart.pdf), ou encore, dès le retrait de son droit d'accès. Le supérieur de l'employé (cadre) ou son représentant (responsable informatique) demande la suspension du code d'identification de cet employé à la DRI. La suppression du code d'identification n'est effectuée que lorsqu'il y a certitude d'absence d'effets dommageables.

Les codes d'identification et les mots de passe sont suspendus après un certain nombre d'essais infructueux.

7. Cadre d'utilisation des ressources informationnelles

7.1 Accès aux ressources informationnelles

L'accès aux ressources informationnelles constitue un privilège. Seuls les usagers, dûment autorisés par le détenteur de la ressource, peuvent avoir accès et utiliser ces technologies, et ce, dans les limites de l'autorisation accordée par le détenteur. L'utilisation de ce privilège est raisonnable et efficace. Le ministère protège l'information qu'il détient par l'attribution d'accès contrôlés et limités à l'exercice des fonctions d'un utilisateur.

Il est interdit d'accéder ou de tenter d'accéder à des fichiers, banques de données, systèmes, réseaux internes ou externes dont l'accès est restreint ou limité à une catégorie spécifique d'utilisateurs.

Le détenteur de ressources informationnelles approuve l'accès à ses ressources en respectant le processus officiel du ministère en matière de gestion des accès aux ressources informationnelles[4] et dans le respect du « *Cadre de référence en matière de PRP*» (http://intranet/Organisation/politique-directive/prp/cadre_reference.htm).

Les demandes d'accès et de modifications d'accès aux systèmes ministériels émanent d'un gestionnaire ou d'une personne dûment habilitée par celui-ci (pilote, copilote, responsable informatique) et sont faites par écrit, soit par courriel ou formulaire (*http://srdri/SST/Formulaire_demande_identifiant_pr_secretaires_v4.htm*).

7.1.1 La demande d'accès aux systèmes

La demande doit comporter les informations suivantes :

- Le nom du requérant ;
- Le nom de la personne qui accèdera à l'information (l'utilisateur) ;
- L'identification du système concerné et autres informations pertinentes s'il y a lieu (transactions, dossiers, etc.) ;
- La spécification de la demande (attribution, ajout, retrait, changement, départ) ;
- Les motifs de la demande.

7.1.2 L'autorisation administrative d'accès aux systèmes

À la réception de la demande, le détenteur ou son représentant habilité (le pilote ou le copilote de système) accepte ou refuse la demande et il en informe le demandeur.

Si la demande implique l'accès à des renseignements personnels, le détenteur s'assure également que l'utilisateur appartient à l'une des catégories de personnes qui, selon la déclaration de fichier existante, auront accès à ces informations dans l'exercice de leur fonction, conformément à l'article 76 de la Loi sur l'accès.

7.1.3 L'intervention technique

Si la demande est acceptée, le détenteur ou la personne habilitée effectue les interventions nécessaires pour rendre l'accès ou la modification de l'accès effectif selon les procédures en vigueur.

---

[4] Utilisation du formulaire " *Demande d'accès aux ressources informationnelles* ".

Lorsque l'accès demandé est disponible ou que les modifications sont effectives, le détenteur avise le demandeur par écrit (courriel, formulaire, note de service).

7.1.4 Sensibilisation de l'utilisateur

Il est de la responsabilité du détenteur et du gestionnaire de l'utilisateur de le sensibiliser aux pratiques spécifiques du système auquel un accès est accordé.

7.2 Révision périodique des accès

Un exercice de révision annuelle des accès (systèmes, services horizontaux, locaux des serveurs et des équipements de télécommunication, identifiants administrateurs) est déclenché par le Responsable de la sécurité de l'information (RSI), en demandant à chaque détenteur une copie du registre des accès dont il est responsable. Chaque détenteur doit aviser le RSI lorsque l'exercice est complété.

Pour les systèmes contenant des informations très sensibles (renseignements personnels, judiciaires, financiers), le détenteur peut déterminer une fréquence de révision plus élevée.

7.3 Modalité d'utilisation

Toute ressource informationnelle est dédiée et réservée uniquement à la réalisation de la mission du ministère et des activités de gestion, de service et de recherche qui en découlent. Elle est utilisée uniquement pour sauvegarder, traiter, consulter ou diffuser de l'information, aux seules fins prévues par la présente Directive.

Dans un contexte de partage équitable des ressources, l'utilisateur ne les monopolise pas ni n'en abuse, entre autres, en effectuant un stockage abusif d'informations.

7.4 Disponibilité de l'information

L'information numérique est accessible en temps voulu et de la manière requise par une personne autorisée, à l'intérieur des balises définies dans « L'offre de services de la DRI » (http://intranet/Organisation/directions/dgsgmt/dri/index.htm).

7.5 Intégrité de l'information

Tout traitement ou manipulation faisant appel à un processus manuel, mécanique ou informatique sur les données et les informations numériques n'altère pas leur intégrité.

7.6 Confidentialité de l'information

L'accès aux informations confidentielles n'est fourni qu'aux personnes autorisées, selon les règles prescrites et conformément aux dispositions applicables en vertu de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) »
(*http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html*)
et de la « *Procédure de mise à jour des déclarations de fichiers et du registre de communication des renseignements personnels* »
(http://intranet/Organisation/politique-directive/prp/Procedure_miseajour.htm).

La collecte de renseignements nominatifs et à caractère confidentiel n'est autorisée que dans la mesure où ces renseignements sont nécessaires à l'exercice des attributions du ministère ou à la mise en œuvre d'un programme dont il a la gestion. De plus, chaque employé du ministère protège l'information recueillie, notamment sur le plan de la confidentialité, conformément aux

dispositions de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* » (*http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html*).

Le citoyen est avisé de l'usage qui sera fait des renseignements nominatifs qu'il fournit et des catégories de personnes qui auront accès à ces informations. Si les renseignements nominatifs servent à d'autres fins que celles pour lesquelles elles sont recueillies, il faut obtenir son consentement spécifique.

Un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle, fourni au ministère pour des fins spécifiques par une entreprise, n'est pas communiqué à d'autres fins sans son consentement.

Une attention particulière est accordée aux renseignements confidentiels transmis par la clientèle du ministère. Les dispositions spécifiques de restriction à la circulation des renseignements, contenues notamment dans un « *Engagement de confidentialité* » du ministère (http://intranet/Outils/techno/securite-informatique/index.htm), sont rigoureusement respectées par le personnel concerné.

Les documents sur différents supports contenant des informations numériques confidentielles (disquettes, cédéroms, bandes magnétiques, DVD, clé USB, etc.) sont protégés contre le vol.

L'utilisateur protège adéquatement l'accès à l'information confidentielle qu'il détient ou à laquelle il accède.

L'utilisateur respecte, lorsqu'il y a lieu, la confidentialité des messages transportés sur le réseau et s'abstient de lire, d'accéder, de modifier ou de détruire tout message, texte, donnée ou logiciel sans l'autorisation de leur propriétaire.

7.7 Chiffrement de l'information

Le chiffrement de l'information, lorsque requis, s'effectue au moyen d'une technologie reconnue par le ministère et l'information est récupérable, selon un processus identifiant les responsabilités des intervenants.

7.8 Conservation, localisation et destruction de l'information numérique

Tout document ou information essentiel(le) est identifié(e) et protégé(e) par des moyens de sécurité appropriés, afin d'en assurer la sauvegarde en tout temps, y compris en situation de crise.

Le ministère est en mesure de localiser l'information durant tout son cycle de vie.

Les renseignements nominatifs, l'information stratégique et confidentielle, ainsi que tout résultat généré par une extraction de cette information, sont **conservés pour un temps limité et détruits de façon sécuritaire**, ou archivés selon les modalités prévues au calendrier de conservation, conformément à la «*Loi sur les archives*» (http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FA_21_1%2FA21_1.htm).

Aucun utilisateur ne peut modifier ou détruire les logiciels, les progiciels, les programmes, les systèmes d'information, une banque de données ou un fichier électronique et les équipements informatiques du ministère, sans l'autorisation préalable des autorités concernées.

Les équipements informatiques déclarés en surplus ou au rebut sont épurés d'information numérique avant leur cession, selon la Directive ministérielle à cet effet « *Directive sur le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-*

informatique ou un support informatique amovible » (http://intranet/Organisation/politique-directive/destruction/index.htm).

7.9 Journalisation

La journalisation est l'enregistrement dans un fichier, du " journal " des opérations informatiques effectuées dans un système afin de garder trace des événements pour vérifications ultérieures ou reconstitution des informations.

Le détenteur détermine les informations à journaliser (accès à un système, transactions, dossiers, etc.). Les utilisateurs des systèmes sont informés de cette journalisation.

Pour les systèmes contenant des renseignements personnels, la journalisation fait l'objet d'une entente entre le détenteur et la responsable de la protection des renseignements personnels au ministère.

Le journal est protégé contre toute altération possible afin d'en préserver l'intégrité.

Les données du journal sont conservées un an. Le détenteur d'un système peut obtenir un délai supplémentaire sur demande.

8. Logiciels et progiciels

8.1 Installation

Tel que défini dans le « *Cadre de gestion des technologies de l'information* » (http://intranet/Organisation/directions/dgsgmt/dri/cgti/index.htm), seul le personnel de la Direction des ressources informationnelles (DRI) dont c'est la tâche et les responsables informatiques peuvent installer et configurer les logiciels et progiciels sur les équipements du ministère dans le respect des normes à cet égard.

Toute installation sur un poste de travail du ministère de logiciels, de progiciels ou de programmes, est préautorisée par le gestionnaire responsable et respecte les normes technologiques en vigueur.

8.2 Outils d'exception

L'utilisation de programmes et de logiciels qui peuvent contourner les mécanismes de sécurité, n'est permise qu'à un nombre restreint d'utilisateurs dûment identifiés et autorisés par le répondant désigné de la sécurité informatique concerné et approuvée par le détenteur des services horizontaux, et ce, dans des circonstances spécifiques (dépannage, installation de nouveau matériel et logiciel, mise à jour de logiciel).

Dans le cadre de ses fonctions, seul le personnel de support des technologies de l'information « Responsable informatique et le personnel de la DRI dédié au support bureautique et du réseau ministériel », est autorisé à utiliser des outils logiciels qui permettent le visionnement à distance de ce qui est affiché à l'écran d'un utilisateur et à prendre le contrôle à distance d'un poste de travail.

8.3 Droits d'auteur

Les logiciels et les progiciels sont protégés adéquatement contre toute utilisation allant à l'encontre des dispositions de la « *Loi canadienne sur le droit d'auteur* (L.R.C., 1985, c. C-42) »

(http://lois.justice.gc.ca/fr/C-42/index.html). Seules les personnes dûment autorisées[5] peuvent utiliser les logiciels et les progiciels du ministère.

Les reproductions de logiciels ou de progiciels respectent les licences d'utilisation, en vertu du droit d'auteur ou sont faites à des fins de copies de sécurité.

Il est interdit de :

- utiliser des reproductions illicites de logiciels ou de progiciels sur les équipements informatiques appartenant au ministère, ou sur tout autre équipement informatique utilisé dans ses locaux ou à tout autre endroit ;
- participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique ;
- contourner les restrictions d'utilisation d'un logiciel ;
- modifier ou détruire un logiciel ;
- reproduire la documentation associée à un logiciel, sans l'autorisation écrite du titulaire du droit d'auteur de ce logiciel ;
- utiliser les équipements et les ressources informatiques et de télécommunication ou le réseau, afin de commettre ou de tenter de commettre une infraction aux lois régissant la propriété intellectuelle.

8.4 Virus informatiques

Tous les postes de travail du ministère sont équipés d'un logiciel antivirus ou autre mécanisme de protection pour contrer la propagation des virus informatiques.

La DRI est responsable de la normalisation de l'antivirus. Des mécanismes de balayage automatique sont en place pour vérifier le niveau de l'antivirus et procéder à sa mise à jour.

L'utilisateur ne désactive pas l'antivirus, ni ne change sa configuration sans autorisation.

9. Équipements informatiques

9.1 Installation

Tel que défini dans le « *Cadre de gestion des technologies de l'information* » (http://intranet/Organisation/directions/dgsgmt/dri/cgti/index.htm), seul le personnel de la DRI dont c'est la tâche et les responsables informatiques peuvent configurer et installer les équipements informatiques du ministère dans le respect des normes à cet égard.

9.2 Protection (accès, perte, dommage)

Les équipements informatiques sont protégés adéquatement contre tout accès non autorisé et contre toute perte ou dommage qui pourrait être causé de façon accidentelle ou délibérée.

Tout ordinateur ayant accès aux informations du ministère est muni d'un écran de veille s'activant automatiquement et protégé par un mot de passe. L'écran de veille est homologué par la DRI.

L'usage d'un ordinateur portatif respecte les « Pratiques recommandées pour accroître la sécurité des ordinateurs portatifs » (http://intranet/Outils/techno/securite-informatique/pratiques_proc.pdf).

---

[5] Voir : Article 3.1 - Personnes visées, page 8.

10. Réseaux informatiques

Le réseau informatique ministériel inclut tous les réseaux locaux au siège social et en région. Il comprend l'ensemble des serveurs, de l'infrastructure technologique et des services de base tels :

- les logiciels utilisés par les employés qui sont pour la plupart, fournis par les réseaux ;
- les imprimantes qui, sauf exception, ne sont accessibles que par le réseau local ;
- le partage des fichiers communs ;
- l'accès à l'Internet, à l'intranet ministériel ainsi qu'au réseau gouvernemental ;
- le courrier électronique.

Le détenteur de ces réseaux est le chef du service du support et des technologies de la DRI.

La gestion des réseaux ministériels se conforme *au « Cadre de gestion des technologies de l'information » (http://intranet/Organisation/directions/dgsgmt/dri/cgti/index.htm).*

Tous les accès internes et externes aux réseaux du ministère sont autorisés par la Direction des ressources informationnelles (DRI). Si un paramétrage est nécessaire, celui-ci se conforme aux normes et procédures en vigueur à la DRI.

L'accès aux réseaux ministériels ne se fait qu'à partir d'un poste de travail configuré et contrôlé par le ministère.

Les réseaux sont protégés contre toute intrusion externe ou interne.

Les différents intervenants (personnel de la DRI, responsables informatiques), respectent les procédures, les canevas et les mécanismes émis par la DRI.

11. Télécommunications et connexité

La télécommunication permet de relier à distance (hors des locaux du ministère), un ordinateur au réseau ministériel et de bénéficier de tous les services informatiques auxquels l'utilisateur a droit.

Seul le personnel autorisé par le détenteur de ce service horizontal est autorisé à :

- brancher les équipements requis à la télécommunication ;
- activer les fonctions nécessaires à son opération ;
- modifier les paramètres de fonctionnement.

Toute intervention se fait selon les normes, directives et procédures de la DRI.

Le maquillage de l'identité (*MAC address*) ou de l'identification (adresse IP ou nom générique) des équipements est interdit.

Les accès sont restreints, lorsque possible, en établissant des domaines logiques séparés par exemple, des réseaux privés virtuels (VPN).

Les salles des serveurs et des télécommunications, de même que les salles de câblage servent exclusivement au regroupement et à l'aménagement du matériel d'infrastructure de télécommunication et de mise en réseau local du bureau. L'accès y est limité au personnel autorisé, de manière à minimiser les risques d'intrusions et de bris d'équipements. À l'intérieur de ces salles, l'accès aux équipements doit être dégagé, de manière à en faciliter l'utilisation et l'entretien. Les salles techniques ne doivent absolument pas servir pour des fins d'entreposage et aucune boîte vide d'équipement, ni autres rebuts ne peuvent y être tolérés.

12. Exploitation et production

12.1 Logiciels d'exploitation

Les paramètres ou options des logiciels d'exploitation[6] sont protégés, de façon à ce que leur sécurité ne soit pas contournée.

12.2 Modification aux systèmes en production

Aucun code d'identification d'utilisateur ne permet de modifier directement les systèmes en production. Les seules modifications permises sont celles qui sont effectuées par les employés du groupe de soutien de l'exploitation, selon le processus de changement en vigueur sur cette plate-forme. (Planification du projet prévue en 2006-2007).

12.3 Logiciels de gestion

Les logiciels de base servant à la gestion et aux contrôles des services informatiques fournis aux utilisateurs, ainsi que tous les nouveaux produits ou produits déjà installés dans les serveurs et les systèmes en production, ont une interface avec le système d'exploitation.

Les procédures exigent que l'imputabilité individuelle soit maintenue pour tout accès par des employés aux services, aux systèmes et aux données.

12.4 Fichiers de système en production

Dans le but de bien distinguer les responsabilités du personnel œuvrant dans les environnements de production et de développement, les fichiers d'un système dans l'environnement de production ne sont accessibles que par les titulaires d'un nombre restreint de codes d'identification, autorisés par le pilote du système en tant que représentant du détenteur. Les modifications effectuées aux fichiers d'un système en production par ces codes d'identification sont retracées en tout temps.

12.5 Protection des commandes d'opération

Sauf exception, seul le personnel autorisé par le détenteur ou le responsable de l'exploitation des systèmes peut exécuter des commandes d'opération pour modifier le statut d'une composante considérée en production et ce, en tout temps.

13. Cadre d'utilisation de l'inforoute

13.1 Modalités d'utilisation

Les services de l'inforoute du ministère sont mis à la disposition du personnel aux seules fins de réaliser plus efficacement les tâches nécessaires à l'accomplissement de ses fonctions.

L'utilisateur de l'inforoute répond aux attentes exprimées dans :

- la «*Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique,* (Loi sur l'administration publique, L.R.Q., c. A-6.01, art. 31)», (http://www.msg.gouv.qc.ca/fr/publications/enligne/environnement/ethique.pdf);
- la « *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (L.R.Q., c. A-2.1) »,

[6] Exemple de logiciels d'exploitation : Opalisrobot, Adlibexpress, Acrobat distiller, etc.

(*http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html*);

- la « Loi concernant le cadre juridique des technologies de l'information (L.Q. 2001, c. 32) », (http://www.msg.gouv.qc.ca/fr/enligne/loi_ti/index.asp);
- le « *Guide de l'inforoute* » du ministère (http://intranet/Outils/guides/inforoutes/index.htm).

13.2 Accès Internet

Outre l'application des règles énoncées au présent document, particulièrement celles de l'article 8, l'accès au réseau Internet est assujetti aux règles suivantes :

- Les accès directs au réseau Internet sont configurés par la Direction des ressources informationnelles et protégés par des coupe-feux ainsi que tout autre mécanisme approprié.
- La Direction des ressources informationnelles identifie les logiciels et plugiciels (*plug-in*) autorisés à accéder à l'Internet ainsi que les services Internet autorisés.
- Les services Internet autorisés comprennent l'usage du service Web, le transfert de fichiers par FTP et le courriel. Tout autre service est au préalable autorisé, contrôlé et sécurisé dans le respect des directives gouvernementales et ministérielles encadrant l'usage de l'Internet.
- L'accès à l'ensemble de l'Internet, à des services ou à des sites est suspendu ou corrigé, si la Direction des ressources informationnelles juge que le réseau interne de l'organisation est exposé à une menace sérieuse ou imminente.
- Les demandes d'accès à l'Internet sont dirigées à la DRI par l'intermédiaire du formulaire « *Demande d'accès aux ressources informationnelles* » (*http://srdri/SST/Formulaire_demande_identifiant_pr_secretaires_v4.htm*), ou par courriel. Les demandes sont envoyées par le gestionnaire de l'utilisateur ou le responsable informatique de l'unité administrative.
- Tous les accès des utilisateurs à l'Internet sont journalisés. Un identifiant réseau disposant d'un accès Internet n'est associé qu'à une seule personne. L'identifiant réseau utilisé lors d'un accès Internet, le service, le site accédé ainsi que la date et l'heure de l'accès, sont conservés deux mois.
- À des fins de saine gestion, des rapports de fréquentation de sites illicites et de téléchargement massif d'informations sont produits quotidiennement par la DRI, qui est mandataire des infrastructures d'Internet. Les situations abusives sont signalées auprès de la Direction des ressources humaines, qui en assure le suivi auprès des supérieurs des utilisateurs concernés.

13.3 Diffusion de l'information du ministère

- La diffusion de toute information par le site Internet du ministère ou les sites dont il a la responsabilité respecte le Guide de diffusion des contenus sur le site Internet ministériel : http://intranet/Outils/guides/inforoutes/guide-diffusion.htm.

14. Normes techniques pour les services horizontaux

Pour chaque service technologique horizontal du ministère, une norme technique de sécurité renforce la " *Politique ministérielle de sécurité de l'information* " à l'égard de ces environnements. Cette norme guide les spécialistes des technologies de l'information dans la configuration de base des équipements et logiciels, l'application des correctifs, la gestion des changements et l'exploitation des environnements qui sont sous leur responsabilité.

15. Développement ou acquisition d'un système d'information

Les besoins en matière de sécurité de l'information numérique et des échanges électroniques de même que la protection des renseignements personnels sont pris en compte dès le début des études menant au développement ou à l'acquisition d'un nouveau système d'information. Le « Cadre de référence en matière de protection des renseignements personnels » est respecté lorsque requis (http://intranet/Organisation/politique-directive/prp/cadre_reference.htm).

16. Ententes de sécurité (ministères, organismes, fournisseurs)

Dans le but de maintenir un niveau de sécurité acceptable pour l'organisation, le ministère :

- intègre aux ententes et aux contrats des dispositions garantissant le respect des exigences de sécurité, comportant les éléments obligatoires déterminés par le Conseil du trésor;
- fait 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 ;
- fait signer le formulaire « Engagement de confidentialité » à toute personne qui n'a pas de lien d'employabilité avec le gouvernement du Québec et qui doit manipuler de l'information numérique du ministère ; ce formulaire est disponible sur l'intranet ministériel dans « Dossiers thématiques\Sécurité informatique\Procédures ».

À cette fin, les ententes incluent, entre autres:

- la nature des services et des informations ;
- les niveaux de service de part et d'autre ;
- les responsabilités réciproques des parties ;
- les règles de sécurité.

L'original de l'entente est conservé par le détenteur.

17. Gestion des incidents

Le ministère dispose d'un processus de gestion des incidents de sécurité qui vise à réduire les conséquences directes et indirectes de tels incidents.

Ce processus permet d'intervenir plus rapidement et plus efficacement pour gérer les crises et assurer le retour normal aux opérations.

Les incidents à effet localisé sont pris en charge par le détenteur ou le gestionnaire concerné. La DRI met à sa disposition les ressources requises pour le supporter dans son action.

Les incidents à effet généralisé sont pris en charge par un comité de crise, dont la composition est définie dans le processus de gestion des incidents. La DRI met à sa disposition les ressources requises pour assurer le retour normal aux opérations.

Tous les incidents nécessitant une intervention (localisée et généralisée), sont rapportés au coordonnateur de la sécurité de l'information numérique, qui avisera le Comité ministériel sur la sécurité de l'information.

L'utilisateur collabore avec la DRI et avec tout gestionnaire et répondant désigné de la sécurité informatique, afin de faciliter l'identification et la correction de tout incident.

18. Vigie de sécurité informatique

Le ministère développe et maintient un niveau de compétence adéquat en sécurité informatique par l'intermédiaire de spécialistes technologiques[7] qui exercent une vigie dans leurs domaines respectifs. Cette approche permet d'anticiper certains problèmes de sécurité, de suivre l'évolution des risques et d'améliorer la capacité d'intervention suite à un incident de sécurité. Par l'entremise du coordonnateur de la sécurité de l'information numérique, cette activité s'intègre au Réseau d'expertise et de vigie gouvernementale pour la sécurité de l'information.

19. Plan de secours

Le ministère dispose de mesures d'urgence, consignées par écrit et éprouvées, en vue d'assurer la remise en opération (dans un délai raisonnable), des systèmes d'information ministériels jugés stratégiques et essentiels en cas de sinistre majeur (ex. : incendie, panne électrique prolongée, inondation, malveillance, etc.). (Mise en place de la relève hors site en 2010-2011).

Chaque détenteur d'un système d'information ministériel ou d'un service horizontal prend les dispositions nécessaires, en collaboration avec les répondants désignés[8] de la sécurité, afin de pouvoir disposer de mesures de secours (mesures de reprise), lui permettant d'assurer la continuité des services essentiels à ses opérations, en cas de sinistre local majeur.

20. Vérification du respect de la Directive

20.1 Processus de vérification

Le ministère peut procéder à toutes les vérifications d'usage qu'il estime nécessaires, pour s'assurer du respect des dispositions de cette directive.

La vérification des informations d'un utilisateur spécifique ou de l'utilisation des ressources informationnelles par celui-ci, peut être effectuée en respectant les dispositions de la « *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels (L.R.Q., c. A-2.1)* », (*http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html*).

S'il a des motifs raisonnables de croire qu'un employé a contrevenu ou contrevient à cette directive, le gestionnaire de l'unité administrative concernée peut procéder à une vérification, après approbation écrite (note ou courriel) de son supérieur immédiat.

La DRI et le détenteur d'un actif informationnel sont autorisés à procéder à une vérification de la sécurité informatique, s'ils ont des raisons de croire à une utilisation non conforme à la présente Directive, des actifs dont ils sont mandataires. Ils peuvent également procéder à l'analyse de leurs résultats. Si une anomalie d'utilisation est constatée, le détenteur en avise, par écrit (note ou courriel), le gestionnaire de l'utilisateur concerné afin que celui-ci normalise la situation.

20.2 Suspension des droits d'accès pendant une vérification

Lorsqu'il y a une raison de croire qu'un utilisateur a contrevenu ou contrevient à cette directive ou aux politiques, règlements, directives, règles d'utilisation, ententes et protocoles pertinents du ministère, ou aux lois ou règlements provinciaux ou fédéraux, son privilège d'accès aux

---

[7] Répondants désignés de la sécurité informatique, responsables informatiques, coordonnateur de la sécurité de l'information numérique.

[8] Répondants désignés de la sécurité : Nous référons ici aux répondants désignés de la sécurité informatique mentionnés à 5.2.5.

équipements et aux ressources informationnelles et de télécommunication, ainsi qu'au réseau, peut être suspendu pour la durée de la vérification. L'utilisateur est prévenu par son gestionnaire que son privilège d'accès est suspendu.

21. Mesures administratives et disciplinaires

L'utilisateur qui contrevient aux dispositions de cette directive peut être l'objet de l'une ou de plusieurs des mesures administratives et disciplinaires suivantes :

- désactivation de son identifiant et de ses mots de passe ;
- interdiction d'utiliser, en totalité ou en partie, les ressources informationnelles ;
- le retrait de ses privilèges d'accès ;
- toute autre mesure administrative ou disciplinaire jugée pertinente.

Conformément au plan ministériel de délégation des pouvoirs en matière de gestion des ressources humaines et en collaboration avec la Direction des ressources humaines (DRH), le gestionnaire de l'unité administrative de l'utilisateur est responsable de voir à l'imposition des mesures administratives ou disciplinaires.

22. Dispositions générales

22.1 Suivi de la Directive

Le suivi de la présente Directive est effectué par le comité ministériel sur la sécurité de l'information.

22.2 Révision périodique

La Directive est révisée périodiquement par le Comité ministériel qui y apporte les ajustements nécessaires, en tenant compte de l'évolution technologique et administrative de l'organisation, du bilan annuel de la Directive et du rapport du vérificateur interne.

22.3 Mesures d'exception – Dérogation

Tout utilisateur peut s'adresser à son gestionnaire pour obtenir l'autorisation d'utiliser les ressources informationnelles et les services reliés à l'inforoute d'une façon non prévue à la présente Directive, dans des **circonstances exceptionnelles**. L'autorisation de la sous-ministre, du sous-ministre adjoint ou du directeur général, le cas échéant, est requise pour toute dérogation demandée. Également, le gestionnaire demandeur avise le coordonnateur de la sécurité de l'information numérique de toute dérogation.

Si les risques associés à la dérogation et les conséquences qui en découlent affectent ou risquent d'affecter l'ensemble des opérations informationnelles du ministère, l'approbation du RSIN est obligatoire. Les risques et les conséquences doivent être clairement exposés par écrit aux signataires concernés (sous-ministre, sous-ministre adjoint, directeur général, gestionnaire, RSIN).

Advenant que la dérogation entraîne la suppression ou la modification à la sécurité telle que définie dans cette directive, les répondants désignés de la sécurité informatique au ministère ne pourront être tenus responsables des conséquences découlant de cette dérogation.

22.4 Date d'entrée en vigueur

La présente Directive entre en vigueur à la date de son approbation par le Comité ministériel de la sécurité de l'information.

22.5 Approbation

Mise à jour approuvée, ce _____ par : _____

AAAA-MM-JJ Bob van Oyen (RSI)

ANNEXE 1 - Lexique

Application informatique : Ensemble organisé de moyens informatiques (traitements, données et interfaces), incluant les progiciels, mis en place pour recueillir, traiter, emmagasiner, communiquer et éliminer l'information dans le but de répondre à un besoin déterminé et de supporter les processus de travail des utilisateurs.

Authentification : Processus permettant d'établir et de vérifier la validité de l'identité déclarée d'une personne, d'un dispositif ou de toute autre entité, ou de garantir l'origine et l'intégrité des messages et autres documents transitant dans un réseau.

Banque de données : Collection d'informations relatives à un domaine défini, regroupées et organisées de façon à en permettre l'accès.

Calendrier de conservation des documents : Outil de gestion qui détermine les périodes d'utilisation et les supports de conservation des documents actifs et semi actifs et qui indique quels documents sont conservés de façon permanente et lesquels sont éliminés.

Chiffrement de l'information : Opération par laquelle on utilise un algorithme pour remplacer un texte en clair, par un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Identifiant : Chaîne de caractères (souvent alphanumérique) qui permet d'identifier de façon unique chaque utilisateur d'un système informatique. Ce code d'identification doit être couplé à un mot de passe confidentiel pour former les codes ou clé d'accès à un système informatique.

Codes d'identification : Ensemble de codes composé généralement d'un code d'identification et d'un mot de passe confidentiel, dont l'utilisation combinée donne accès à un système informatique.

Comité de crise : Équipe formée de cadres supérieurs visant à gérer les crises à impacts majeurs sur l'organisation. Assigne les ressources nécessaires, coordonne les actions entre les intervenants internes et externes.

Commande d'opérations : Le statut d'une composante en production peut être modifié par l'utilisation de facilités spécialisées comme DMLO sur les ordinateurs centraux.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes autorisées.

Continuité : Propriété qu'ont les ressources informationnelles d'être accessibles de la manière requise (sans interruption, délai ou dégradation) et utilisables au moment voulu.

Contrôle d'accès : Processus par lequel les données d'identification et d'authentification que fournit une personne sur elle-même pour avoir accès à une zone sécurisée, à un système d'information ou à une ressource informationnelle sont comparées à des valeurs de référence définies, permettant ainsi l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique.

Courriel : Aussi appelé courrier électronique, messagerie électronique ou « *email* », le courriel est un service de correspondance qui permet aux utilisateurs d'échanger des messages écrits d'ordinateur à ordinateur, parfois accompagnés de fichiers, par l'intermédiaire de serveurs agissant comme boîtes postales, à travers un réseau de téléinformatique.

Cycle de vie de l'information : Période de temps couvrant toutes les étapes d'existence de l'information dont celles de sa création, de son enregistrement, de son traitement, de sa diffusion, de sa conservation et de sa destruction.

Détenteur : Le détenteur est un gestionnaire à qui a été confié la propriété d'un système par la sous-ministre et qui agit à titre de responsable désigné de la protection de ce système.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Document : Toute information délimitée et structurée de façon tangible ou logique, selon le support qui la porte, et qui est intelligible sous forme d'écrit, d'image ou de son. Le document peut être rédigé au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles 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 délimitation et la structuration de l'information qui y est inscrite.

Évolution : Réévaluation périodique des pratiques et solutions techniques retenues en matière de sécurité afin de tenir compte des changements organisationnels et technologiques qui peuvent survenir.

Fournisseur : Corporation, société, coopérative, personne physique, unité administrative ou tout fonds spécial du gouvernement qui fait affaire avec le ministère en vue de lui fournir des services ou des biens informatiques.

Identification : Action permettant d'attribuer un identifiant à un individu ou à un dispositif matériel.

Incident de sécurité : Tout événement ou action ayant une répercussion négative sur la sécurité de l'information et des ressources informationnelles. Par exemple, les virus, l'intrusion, l'usurpation d'identité, etc.

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

Inforoute : Réseau étendu d'information à haut débit et à grande vitesse, capable de transmettre des données de toutes sortes, notamment des données multimédias, et destiné à jouer le rôle d'infrastructure globale de communication au service de l'ensemble des populations, sur les plans national et international.

Intégrité : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation.

Internet : Réseau informatique mondial d'échange d'information numérique, constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole

de communication TCP/IP (*Transmission Control Protocol/Internet Protocol*) et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

Intranet : Réplique du réseau Internet à l'intérieur d'une organisation. Utilisant les mêmes protocoles et les mêmes logiciels que le réseau Internet, l'intranet d'une entreprise facilite la communication et l'échange d'information entre les membres du personnel. L'accès à ce réseau est protégé et seul les employés d'une organisation peuvent y accéder.

Logiciel : Ensemble commercialisé de programmes et procédés relatifs au traitement informatique des données.

Logiciel antivirus : Logiciel de sécurité qui procède, automatiquement ou sur demande, à l'analyse des fichiers et de la mémoire d'un ordinateur, soit pour empêcher toute introduction de virus, soit pour détecter et éradiquer tout virus dans un système d'information.

Logiciel de gestion : Ce type de logiciel peut être intégré au logiciel d'exploitation comme avec Windows NT ou extérieur à celui-ci tel « Radius ».

Menace : Événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique.

Mesure de sécurité : Mécanisme technique et/ou administratif qui vise à assurer, partiellement ou totalement, la protection des ressources informationnelles du ministère contre une ou plusieurs risques informatiques, et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à minimiser les pertes qui pourraient en résulter.

Mot de passe : Code secret prenant la forme d'une chaîne de caractères choisie par l'utilisateur et qui, lorsque couplé au code d'identification de cet utilisateur, permet de former la clé d'accès unique aux ressources informationnelles du ministère pour cet utilisateur particulier. Le mot de passe ne doit pas être divulgué à une autre personne, ni être inséré dans une procédure automatisée d'entrée en communication à un système d'information.

Plan de secours : Plan permettant de prendre les mesures nécessaires en vue d'assurer, sur site ou hors site, la reprise des services informatiques jugés essentiels à la suite d'un sinistre ou d'une interruption.

Plugiciel : Logiciel d'application complémentaire qui, associé à un navigateur Web, entre automatiquement en action en présence d'un objet multimédia, et ce, sans que l'utilisateur ait à intervenir. Le plugiciel constitue un « plus » en augmentant les performances du logiciel principal.

Politique : Document d'orientation qui couvre l'ensemble d'un domaine et qui sert de cadre de référence. On y expose une problématique puis on y définit les lignes directrices et les objectifs stratégiques à atteindre. (Source : Office de la langue française).

Poste de travail : Micro-ordinateur mis à la disposition d'un utilisateur de manière à permettre le traitement informatique des informations qu'il doit créer, consulter ou transformer.

Progiciel : Ensemble complet et documenté de programmes informatiques développés par une firme spécialisée qui sert à répondre aux besoins d'une application similaire à plusieurs organisations.

Renseignements confidentiels : Renseignements qui ont la propriété de comporter une ou plusieurs restrictions et de n'être accessibles qu'aux personnes autorisées et pour les fins accordées.

Renseignements personnels ou nominatifs : Renseignements qui concernent une personne physique et permettent de l'identifier (entre autres, le nom, l'adresse civique, les numéros d'assurance sociale, de permis de conduire, etc.).

Réseau : Ensemble des postes de travail, reliés ou non à un ou plusieurs serveurs, qui ont pour fonction de se partager ou de traiter de l'information.

Ressources informationnelles : Tout logiciel, tous les équipements informatiques ou combinaison de ces éléments utilisés par le ministère pour recueillir, emmagasiner, traiter, communiquer, reproduire et protéger l'information numérique.

Serveur : Ordinateur permettant de rendre accessibles, aux postes de travail qui y sont reliés, des données, des logiciels et des applications informatiques.

Sinistre : Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des dommages graves aux technologies de l'information du ministère de sorte qu'elles ne sont plus opérantes et totalement inutilisables.

Système d'information : Ensemble de programmes informatiques qui contribuent au traitement et à la circulation de l'information numérique au ministère.

Virus : Programme informatique infectieux, inséré dans un système informatique (ordinateur) dans le but d'exercer une action nuisible à son environnement (modification ou destruction de fichiers, effacement du disque dur, allongement du temps de traitement, manifestations visuelles ou sonores, etc.). Les virus peuvent se multiplier et infecter d'autres programmes et données d'un ordinateur ou le secteur de démarrage du disque dur et des disquettes de même que le contenu de tout autre support d'information électronique qui lui est relié.

Web ou WWW : Ensemble de serveurs reliés par le réseau Internet avec le protocole HTTP (« *HyperText Transfer Protocol* »), offrant aux utilisateurs la recherche et l'accès à de l'information en format hypertexte programmée avec le langage HTML (« *HyperText Markup Language* »). Le Web désigne le service le plus en vogue d'Internet et celui qui évolue le plus rapidement. On y trouve des sites d'information, de divertissement, de promotion et des applications du commerce électronique.

Développement durable,
Environnement
et Parcs
Québec

Direction générale des technologies de l'information

DIRECTIVE MINISTÉRIELLE DE SÉCURITÉ LIÉE À L'UTILISATION DES TERMINAUX SANS FIL

(Assistants numériques personnels (BlackBerry, Palm et autres), téléphones cellulaires et ordinateurs portables)

(Version 2.0)

Sécurité de l'information

Québec, Décembre 2011

TABLE DES MATIÈRES

Mise à jour : 14 mai 2010 (Robert Parent)
Août 2011 (Guy Carreau – Robert Parent)
Décembre 2011 (Robert Parent)

1. CONTEXTE

L'utilisation des terminaux sans fil a pour but l'amélioration de la qualité des services et l'accroissement de la productivité. Or, l'information traitée et emmagasinée sur ces équipements peut renfermer des renseignements nominatifs ou confidentiels et stratégiques pour le Ministère et doit donc faire l'objet d'une utilisation et d'une protection adéquates considérant que l'information peut se retrouver à l'extérieur des bureaux.

Afin d'assumer pleinement ses responsabilités quant à la sécurité de l'information et d'intégrer la gestion de la sécurité dans ses processus d'affaires, le Ministère a élaboré la présente directive de sécurité liée à l'utilisation des terminaux sans fil.

Cette directive a été adaptée à partir de la « *Directive ministérielle de sécurité liée à l'utilisation des terminaux sans fil (du type BlackBerry, Palm et autres)* » émise par le ministère des Services gouvernementaux le 15 décembre 2006. Elle énonce les technologies et types d'appareils permis et supportés par la Direction générale des technologies de l'information (DGTI) du Ministère ainsi que leur mode d'implantation et d'opération.

2. DÉFINITIONS

Terminaux sans fil du type Blackberry, Treo et autres :

Assistant numérique personnel (ANP) est une traduction de Personal Digital Assistant (PDA). Ordinateur de poche, servant de complément à l'ordinateur de bureau ou à l'ordinateur portatif, qui intègre de multiples fonctions de gestion qui lui permettent d'être utilisé comme outil de travail pendant les déplacements d'une personne. Entre autres, ces appareils regroupent les carnets d'adresses, le courriel et ses pièces jointes, l'agenda électronique ainsi que le téléphone cellulaire.

Utilisateur :

Personnel autorisé par son gestionnaire à utiliser un terminal sans fil dans le cadre de ses fonctions.

3. OBJECTIFS

Cette directive identifie le champ d'application et précise la position du Ministère relativement à la sécurité, à la protection, aux échanges et à la conservation des informations reliées à l'utilisation des terminaux sans fil.

La présente directive a pour objectifs de :

- doter le Ministère et les utilisateurs de terminaux sans fil d'un cadre référentiel leur permettant d'assurer la sécurité et la protection de renseignements personnels, confidentiels et stratégiques transitant et emmagasinés sur leurs terminaux sans fil;
- sensibiliser le personnel aux risques inhérents à l'utilisation non protégée des terminaux sans fil;
- préciser les responsabilités des différents intervenants au niveau de la disponibilité, de l'intégrité et de la confidentialité de l'information sur leurs terminaux sans fil;
- diminuer les risques potentiels liés à une utilisation non sécurisée des terminaux sans fil. Soulignons, entre autres :
    - divulgation et fuite de renseignements personnels et confidentiels (ex. : numéros de téléphone confidentiels) ou des renseignements stratégiques (ex. : orientations gouvernementales et ministérielles à l'état de projet, projets de mémoire, projets du Conseil du trésor en cours d'élaboration);;
    - usurpation d'identité par la diffusion de l'information dans des sites non pertinents;
    - utilisation inappropriée ou illicite des appareils par une tierce personne.

4. CADRE LÉGAL ET ADMINISTRATIF

Les principales lois et directives relatives à l'administration publique servant de référence sont :

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)
- Loi sur l'Administration publique (L.R.Q., c. A-6.01)

- Loi sur les archives (L.R.Q., c. A-21.1)
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1)
- Loi sur le droit d'auteur (L.R.C., (1985), C-42)
- Code criminel (L.R.C., (1985), C-46)
- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12)
- Règlement sur l'éthique et la discipline dans la fonction publique (L.R.Q., c. F-3.1.1 a. 126, par. 1 à 3)
- Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (CT 198872)
- Directive sur la sécurité de l'information gouvernementale (CT 203560)
- Directive sur la gestion des ressources informationnelles (CT 203887 modifié par le CT 205125 du 18 juin 2007)
- Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible (CT 193953 modifié par le CT 199891 du 27 mai 2003)
- Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique (CT 197638 modifié par les CT 203887 et 203888 du 13 juin 2006)
- Politique et Directive ministérielles sur la sécurité de l'information numérique et des échanges électroniques.

5. CHAMP D'APPLICATION

La directive s'applique en tout temps à tout utilisateur qui utilise des terminaux sans fil ainsi qu'à toute personne qui, par engagement contractuel, est dûment autorisée à utiliser les terminaux sans fil reliés au réseau du Ministère.

Par terminal sans fil, nous faisons référence aux assistants numériques personnels de type BlackBerry, Palm et autres, aux téléphones cellulaires et aux ordinateurs portables.

6. MODALITÉS D'UTILISATION

Dans le cadre de l'utilisation d'assistant numérique personnel :

L'infrastructure officielle du Ministère pour les assistants numériques personnels est celle du Blackberry sur le réseau Rogers sans fil supportée par un serveur BES (BlackBerry Entreprise Server) opéré et géré par la DGTI. Seuls ces appareils sont supportés pour la synchronisation sans fil avec les données du réseau ministériel. À moins de conditions de non couverture cellulaire, les appareils doivent être activés sur le réseau de Rogers sans fil. Ces appareils sont enregistrés dans le serveur BES et sont soumis à des politiques de sécurité mises à jour périodiquement. Ces politiques permettent de contrôler les paramètres de sécurité fixés par la DGTI, notamment :

- obligation d'un mot de passe;
- longueur du mot de passe;
- fréquence de changement du mot de passe;
- activation et délai de verrouillage automatique;
- applications permises.

De plus, des commandes d'effacement peuvent être envoyées à distance à travers le réseau cellulaire aux appareils lors de perte ou de vol.

Les autres types d'assistants numériques personnels (Palm, HP, téléphones cellulaires évolués, etc.), ne sont pas supportés par la DGTI. Il appartient à l'utilisateur d'appliquer les principes de sécurité mentionnés dans cette directive.

Dans le cadre de l'utilisation d'ordinateurs portables :

Les ordinateurs portables appartenant au Ministère ne sont pas paramétrés ni attestés par la DGTI pour se raccorder à des réseaux locaux sans fil. Il peut cependant y avoir des besoins spécifiques pour ce genre de raccordement, surtout pour l'accès à l'Internet à la maison, à l'hôtel, etc. Ces exceptions doivent faire l'objet d'une autorisation du gestionnaire et être rapportées à la DGTI pour consignation.

Lors du branchement sans fil à l'Internet, l'installation de l'ordinateur doit rencontrer les points suivants :

- le pare-feu est actif;
- le poste est à jour en ce qui concerne les rustines de sécurité d'un logiciel anti-virus.

Afin que les différentes composantes de sécurité du poste soient à jour, il doit être raccordé directement au réseau ministériel dans un bureau du Ministère de façon régulière.

Pour des raisons de sécurité, il est strictement interdit d'utiliser les branchements sans fil à l'Internet à l'intérieur des bureaux du Ministère ou d'utiliser des dispositifs sans fil raccordés au réseau ministériel.

Pour l'accès à Internet :

L'accès à l'Internet doit se faire dans le respect de la directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique : http://www.rpg.tresor.qc/pdf/1-1-1-5.pdf. Ces accès sont contrôlés et journalisés selon les mêmes règles que les accès effectués à partir du réseau local.

7. PROTECTION DES INFORMATIONS

Le Ministère a la responsabilité d'assurer la protection de ses informations au niveau de la disponibilité, l'intégrité et la confidentialité, peu importe le média utilisé, et ce, tout au long de son cycle de vie. Cette responsabilité incombe également aux divers intervenants.

De plus, l'utilisation de terminaux sans fil respecte les principes de sécurité émis par les politiques et directives gouvernementales et ministérielles.

À titre préventif, il est important de mentionner que :

- La conservation du courrier électronique et de ses pièces jointes, qui contiennent des informations nominatives ou des renseignements confidentiels et stratégiques, doit être limitée à l'essentiel et les informations doivent être effacées lorsque leur présence n'est plus requise sur le terminal sans fil afin de minimiser les risques lors de perte ou de vol de l'appareil.
- Lors des conversations téléphoniques avec des terminaux sans fil, l'information nominative et les renseignements confidentiels et stratégiques du Ministère doivent faire l'objet d'une grande vigilance.

8. RESPONSABILITÉS

8.1 Sous-ministre

La sous-ministre approuve la présente directive de sécurité liée à l'utilisation des terminaux sans fil gérés par le Ministère.

8.2 Comité ministériel sur l'accès, la sécurité de l'information et la protection des renseignements personnels

Le suivi de la présente directive est effectué par le Comité ministériel sur l'accès, la sécurité de l'information et la protection des renseignements personnels (CMASI-PRP). Les modifications, le cas échéant, sont approuvées par la sous-ministre.

Le CMASI-PRP a statué que « **L'utilisation du mot de passe, comme mesure de sécurité, est obligatoire. Il n'y aura aucune dérogation pour qui que ce soit** ».

8.3 Utilisateurs

L'utilisateur d'un terminal sans fil est responsable de la protection de l'information lors de l'utilisation de l'appareil, du traitement ainsi que de la conservation sécuritaire des données qu'il contient, et ce, sous toutes ses formes. De plus, il doit procéder à l'effacement de l'information emmagasinée sur son terminal sans fil, lorsque cette dernière n'est plus requise.

L'utilisateur doit protéger l'accès à son terminal sans fil, en utilisant les moyens mis à sa disposition (mot de passe, verrou, écran de veille, etc.).

L'utilisateur s'engage à respecter les droits d'auteur concernant les logiciels installés sur le terminal sans fil, à ne pas modifier la configuration des terminaux utilisés, à ne pas désactiver les mesures de sécurité et à ne pas installer de nouveaux logiciels sans l'autorisation écrite de son gestionnaire.

L'utilisateur s'engage à ne pas télécharger, reproduire électroniquement ou transmettre à un tiers tout élément protégé par droits d'auteur, marques de commerce ou brevets, sauf s'il émane d'un expéditeur qui aurait implicitement donné son autorisation ou si une autorisation écrite a été donnée, au préalable, par le propriétaire de ces droits.

L'utilisateur qui constate la disparition de son terminal sans fil doit informer immédiatement son gestionnaire et son responsable informatique conformément à la « *Procédure de gestion des incidents de sécurité informatique* ». Particulièrement dans le cas de la disparition d'un terminal BlackBerry, la Direction générale des technologies de l'information doit être contactée, sans délai, afin de le désactiver.

L'utilisateur a la responsabilité de retourner le terminal sans fil lorsqu'il quitte le Ministère, si celui-ci est la propriété du Ministère.

8.4 Direction générale des technologies de l'information

La Direction générale des technologies de l'information est responsable de l'acquisition et de la distribution des assistants numériques personnels de type Blackberry.

Elle assure également le support technique pour les téléphones cellulaires.

La Direction générale des technologies de l'information est responsable de fournir l'encadrement, le soutien technique, de même que les moyens opérationnels pour assurer la disponibilité, l'intégrité et la confidentialité de l'information dans le cadre de l'utilisation des terminaux sans fil.

Seuls les appareils BlackBerry et les ordinateurs portables font l'objet d'un support technique par la DGTI. Les autres types d'assistants numériques personnels (Palm. HP, téléphones cellulaires évolués, etc.), bien qu'utilisés au Ministère, ne sont pas supportés par la DGTI car elle ne peut avoir de contrôle sur la sécurité de ces appareils (mot de passe, verrouillage, applications, effacement, etc.) et ne peut donc garantir la sécurité des informations qu'ils contiennent. Cependant, la DGTI offre une assistance technique de premier niveau pour l'installation initiale de la synchronisation des informations à partir d'un poste de travail.

La DGTI s'assure de l'effacement de l'information dans les cas suivants :

- un BlackBerry dans les situations d'urgence (perte ou vol);
- un BlackBerry ou un ordinateur portable dans les cas de transfert de terminaux d'un utilisateur à un autre;
- un BlackBerry ou un ordinateur portable avant l'expédition de l'appareil au recyclage ou au rebut.

Concernant l'utilisation d'Internet sans fil dans les hôtels, la DGTI n'offre pas de service de dépannage étant donné la diversité des services et des installations impliqués.

La DGTI est responsable de maintenir à jour un inventaire ministériel pour les assistants numériques personnels.

8.5 Responsable de la sécurité de l'information numérique

Le responsable de la sécurité de l'information numérique (RSIN) s'assure de l'élaboration, de l'approbation, de la mise à jour, de l'application et du respect de la présente directive. Il est assisté par le coordonnateur de la sécurité de l'information numérique qui a pour responsabilité, notamment, la tenue d'un registre où sont consignés tous les cas de dérogation à la directive.

8.6 Gestionnaire/détenteur

Le gestionnaire autorise l'acquisition d'un terminal sans fil par le personnel de son unité administrative et s'assure de son utilisation conformément à cette directive.

Si un gestionnaire autorise à un employé un autre type d'appareil que ceux supportés par la DGTI, il est responsable de la sécurité de l'information s'y retrouvant et sera le répondant lors d'incidents.

Le gestionnaire a la responsabilité de récupérer le terminal sans fil de l'employé sous sa responsabilité lorsqu'il quitte le Ministère.

Le gestionnaire de l'unité administrative de l'utilisateur est responsable de voir à l'imposition des mesures administratives ou disciplinaires, s'il y a lieu, conformément au plan ministériel de délégation des pouvoirs en matière de gestion des ressources humaines.

9. DISPOSITIONS GÉNÉRALES

9.1 Propriété de l'appareil et de l'information

Les terminaux sans fil fournis par le Ministère demeurent la propriété de ce dernier et peuvent être récupérés en tout temps afin d'effectuer des mises à jour, des vérifications et des contrôles.

Toute information emmagasinée sur les terminaux sans fil des utilisateurs est réputée constituer une information à laquelle le Ministère a accès.

Le Ministère se réserve le droit d'ouvrir, de récupérer, de lire les courriers électroniques, messages vocaux ou fichiers électroniques afin d'exécuter la maintenance ou de repérer des communications qui ne seraient pas conformes aux conditions d'utilisation prescrites par la présente directive.

La DGTI applique automatiquement un processus de journalisation sur les informations qui transitent par les terminaux sans fil. À cet effet, les journaux produits (journal d'appels téléphoniques, courrier, etc.) demeurent la propriété du Ministère.

9.2 Processus de vérification

Le Ministère peut procéder à toutes les vérifications d'usage qu'il estime nécessaires pour s'assurer du respect des dispositions de cette directive.

La vérification des informations d'un utilisateur spécifique ou de l'utilisation des ressources informationnelles par celui-ci, peut être effectuée en respectant les dispositions de la « *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels (L.R.Q., c. A-2.1)* », (http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html).

La DGTI et le détenteur d'un actif informationnel sont autorisés à procéder à une vérification de la sécurité informatique, s'ils ont des raisons de croire à une utilisation non conforme à la présente directive, des actifs dont ils sont mandataires. Ils peuvent également procéder à l'analyse de leurs résultats. Si une anomalie d'utilisation est constatée, le détenteur en avise, par écrit (note ou courriel), le gestionnaire de l'utilisateur concerné afin que celui-ci normalise la situation.

9.3 Mesures administratives ou disciplinaires

L'utilisateur qui contrevient aux dispositions de cette directive peut être l'objet de l'une ou de plusieurs des mesures administratives et disciplinaires suivantes :

- désactivation de son identifiant et de ses mots de passe;
- interdiction d'utiliser, en totalité ou en partie, les ressources informationnelles;
- retrait de ses privilèges d'accès;
- toute autre mesure administrative ou disciplinaire jugée pertinente.

Conformément au plan ministériel de délégation des pouvoirs en matière de gestion des ressources humaines et en collaboration avec la Direction des ressources humaines (DRH), le gestionnaire de l'unité administrative de l'utilisateur est responsable de voir à l'imposition des mesures administratives ou disciplinaires.

9.4 Mesures d'exception - dérogation

Tout utilisateur peut s'adresser à son gestionnaire pour obtenir l'autorisation d'utiliser les terminaux sans fil d'une façon non prévue à la présente directive, dans des circonstances exceptionnelles. L'autorisation de la sous-ministre, du sous-ministre adjoint ou du directeur général, le cas échéant, est requise pour toute dérogation demandée. Également, le gestionnaire demandeur avise le coordonnateur de la sécurité de l'information numérique de toute dérogation.

Si les risques associés à la dérogation et les conséquences qui en découlent affectent ou risquent d'affecter l'ensemble des opérations informationnelles du Ministère, l'approbation du RSIN est obligatoire. Les risques et les conséquences doivent être clairement exposés par écrit aux signataires concernés (sous-ministre, sous-ministre adjoint, directeur général, gestionnaire, RSIN).

Advenant que la dérogation entraîne la suppression ou la modification à la sécurité telle que définie dans cette directive, les répondants désignés de la sécurité informatique au Ministère ne pourront être tenus responsables des conséquences découlant de cette dérogation.

10. APPROBATION ET ENTRÉE EN VIGUEUR

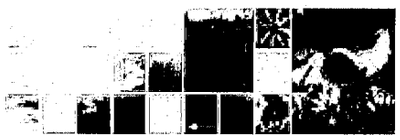
La présente directive entre en vigueur à la date de son approbation par la sous-ministre.

Approuvée le : _____

La sous-ministre : _____

Mise à jour : 1 avril 2010 (Robert Parent)
15 décembre 2011 (Robert Parent)

Développement durable, Environnement et Lutte contre les changements climatiques
Québec



Introduction à la sécurité de l'information

Définitions et notions de bases en sécurité de l'information - Initiation aux principes de la sécurité de l'information numérique et des technologies de l'information

Introduction à la sécurité

Définitions et notions de bases

Conseils pratiques

Définitions et notions de bases

Qu'est-ce que la sécurité de l'information?

C'est un processus visant à protéger les données contre l'utilisation, la diffusion, la destruction, la modification ou l'accès non autorisés.

Portée de la sécurité de l'information

La sécurité de l'information s'adresse à tous les types de supports d'information autant le numérique que le papier, également touche la sécurité physique.

Particularités

La sécurité de l'information implique la mise en place d'un ensemble de mesures de protection, de techniques et de règles d'utilisation, le déploiement d'outils technologiques de sécurité et l'élaboration de politiques de sécurité.

Couvre l'ensemble des aspects qui touchent, de près ou de loin aux processus, à l'équipement, et au personnel qui utilise, traite ou modifie l'information reliée à l'organisation, ses clients, partenaires et employés.

L'objectif de la sécurité de l'information consiste à préserver les critères de confidentialité, d'intégrité et de disponibilité assignés à l'information ou à un actif informationnel lui étant associé.

Qu'est-ce que le DIC?

- **Disponibilité :**
  Propriété d'une information d'être accessible en temps voulu et de la manière requise, par une personne ou une entité autorisée.

- **Intégrité :**
  Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation.

- **Confidentialité :**
  Propriété d'une information de n'être accessible qu'aux personnes autorisées.

Cycle de vie de l'information

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.

Données sensibles

Les renseignements personnels et confidentiels ou stratégiques du Ministère.

Pourquoi se préoccuper de la sécurité de l'information

Le Ministère a la responsabilité d'assurer la sécurité de l'information qu'il détient, qu'il traite et d'utiliser les technologies de l'information dans le respect des règles.

Parce que les données du Ministère, souvent de nature sensible sont davantage exposées à des risques et des menaces compte d'une évolution constante des technologies de l'information et d'une utilisation accrue. En l'absence de mécanises et moyens de protection, la perte ou le vol d'informations pourraient en tout temps causés des préjudices et nuire à l'image du Ministère.

Risques et conséquences	
Risques	**Conséquences**
Accès par des personnes non autorisées	Divulgation des renseignements confidentiels Altération, perte, destruction ou vol d'informations Fraude, sabotage Interruption de services
Introduction de virus ou de codes malicieux	Modification ou destruction de données Transmission involontaire d'informations Interruption des opérations Dégradation du fonctionnement des

	équipements Investissement de ressources dans le rétablissement des services
Divulgation d'informations confidentielles	Perte de confiance Préjudice causé aux personnes Sanction ou poursuite

Conseils pratiques

Mot de passe

- N'utilisez jamais un renseignement personnel
- Créez un mot de passe d'un minimum de 8 caractères formé d'une combinaison de chiffres, de lettres ou d'autres caractères
- Changez régulièrement votre mot de passe
- Mémorisez votre mot de passe
- Conservez en tout temps votre mot de passe confidentiel

Sécurité des courriels

- Évitez d'ouvrir un courriel ou une pièce jointe dont l'objet semble étrange ou l'expéditeur douteux
- Refusez de participer à une chaîne de lettres et évitez les sites douteux
- N'utilisez pas le courriel du Ministère à des fins personnelles
- Ne pas redirigez vos courriels du bureau à votre messagerie personnelle

Sécurité des données

- Évitez de transporter des données sensibles ou confidentielles à l'extérieur des bureaux du Ministère, au besoin, utilisez les mécanismes de chiffrement des données ou médias appropriés.
- Enregistrez vos fichiers sur les serveurs du Ministère (ainsi des copies de sauvegarde de vos données seront effectuées).
- Évitez l'enregistrement de données confidentielles sur votre disque local.

Sécurité physique

- Verrouillez votre poste de travail avant de quitter votre bureau
- Utilisez un écran de veille protégé par un mot de passe
- Fermez votre session réseau à la fin de votre journée de travail
- Conservez vos disquettes et autres supports amovibles et contenant des renseignements confidentiels dans des endroits sécuritaires
- Protégez adéquatement vos documents de type papier contenant des renseignements confidentiels à toutes les étapes de leur conservation, de leur transmission et de leur destruction
- Accompagnez les visiteurs dans les zones sécurisées

Retour à l'index

Mise à jour : 2015-01-13

Source : Lucie Racine
Direction générale des technologies de l'information

418 521-3838, poste 4254

Québec