Société d'habitation Québec

Politique sur l'accès, la sécurité de l'information et la protection des renseignements personnels

Version approuvée par le CA du 5 février 2010

La présente politique a été élaborée par le Comité sur l'accès, la sécurité de l'information et la protection des renseignements personnels (CASIPRP) de la Société d'habitation du Québec.

ÉQUIPE DE RÉDACTION :

Secrétariat de la Société
M^{e} Marilyn Thibault
M^{me} Guylaine Marcoux
M^{me} Lynda Chabot

Horus information et technologie inc.
M. Benoît Jourdain

Pour tout renseignement supplémentaire ou commentaire concernant cette politique, veuillez communiquer avec :

Société d'habitation du Québec
Bureau du président-directeur général
Aile Saint-Amable, 3^{e} étage
1054, rue Louis-Alexandre-Taschereau
Québec (Québec) G1R 5E7
Téléphone : 418 644-2111

TABLE DES MATIÈRES

1 INTRODUCTION

La Société d'habitation du Québec détient de l'information sur différents supports, et ce, durant tout le cycle de vie de celle-ci. Cette information est nécessaire et a une importance stratégique pour le déroulement des activités de la Société.

Toute information détenue par la Société impose que l'organisation se donne des règles concernant l'accès et la sécurité de celle-ci ainsi que la protection des renseignements personnels.

2 OBJECTIFS DE LA POLITIQUE

La présente politique a pour objet d'établir les principes directeurs et les lignes de conduite à suivre en matière d'accès à l'information, de protection des renseignements personnels (PRP) et de sécurité de l'information (SI), et ce, dans le respect des lois, règlements et directives gouvernementales applicables en la matière.

3 CHAMP D'APPLICATION

3.1 Personnes concernées

Cette politique s'adresse à tout le personnel de la Société. Elle concerne également toutes les personnes appelées à utiliser les actifs informationnels de l'organisation ou à accéder aux renseignements qu'elle détient.

3.2 Actifs visés

Tous les actifs informationnels de la Société sont visés par la présente politique quel que soit le support utilisé pour les porter.

4 CADRE LÉGISLATIF, RÉGLEMENTAIRE ET ADMINISTRATIF

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), la Société est tenue d'adopter et d'appliquer des mesures administratives permettant d'encadrer les privilèges, restrictions et procédures en matière d'accès à ses documents. Elle doit également protéger les renseignements personnels en tenant compte de leur caractère confidentiel, de leur collecte, de leur conservation et de leur utilisation, tout en considérant aussi l'établissement et la gestion des fichiers.

La Société doit aussi appliquer la Directive sur la sécurité de l'information gouvernementale ainsi que la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1-1) en matière de SI et de sécurité juridique de la communication effectuées au moyen de documents, peu importe le support.

L'annexe 1 contient la liste des lois, des règlements et des directives dont la Société doit tenir compte dans le cadre de la mise en œuvre des mesures destinées à assurer l'accès à l'information, la PRP et la SI. Les différentes définitions applicables dans la présente politique sont données à l'annexe 2.

5 PRINCIPES DIRECTEURS

Les principes directeurs de la Société pour l'accès à l'information et la PRP sont :

- La collecte : la Société doit, lorsqu'elle recueille des renseignements personnels, respecter la règle de nécessité en vertu de laquelle un organisme public ne peut recueillir que les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. En vertu de cette règle, la Société a aussi l'obligation d'informer la personne concernée des raisons de la collecte et du traitement qui sera fait de l'information recueillie.

  La personne concernée a un droit de regard et de rectification sur les renseignements qu'un organisme public a recueillis.
- L'accès : la Société doit limiter la circulation des renseignements personnels qu'elle a recueillis. Seules les personnes qui ont besoin des renseignements dans le cadre de leurs fonctions et de leurs activités doivent y accéder.
- L'utilisation : la Société peut utiliser des renseignements personnels à d'autres fins que celles prévues, si la personne concernée a donné son consentement ou qu'une loi l'autorise.
- La communication : dans le cas des communications autorisées par les personnes concernées, la Société doit s'assurer que le consentement est valide et que la communication des renseignements s'effectue de manière à préserver leur caractère confidentiel.
- La détention et la conservation : la Société doit veiller à ce que les renseignements personnels qu'elle conserve soient à jour, exacts et complets, afin de servir aux fins prévues. Elle doit aussi s'assurer de gérer de manière sécuritaire l'ensemble des renseignements personnels qu'elle détient.
- La destruction et l'archivage : la Société doit détruire un renseignement lorsque l'objet pour lequel il a été recueilli est accompli et que le calendrier de conservation est respecté.

Les principes directeurs de la Société pour la sécurité de l'information sont :

- La responsabilité et l'imputabilité : l'efficacité de la SI exige l'attribution claire de responsabilités à tous les membres du personnel de la Société, qu'importent leurs fonctions. Elle doit permettre une reddition de comptes adéquate en accord avec le cadre légal.

- L’évolution : les pratiques et les solutions retenues en matière de SI 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 SI 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 SI doit être soutenu par une prise en charge des enjeux éthiques ayant pour but d’assurer la régulation des conduites et la responsabilisation individuelle. Cette approche vise à assurer l’intégrité, et l’efficacité du personnel de la Société dans toutes ses activités, et ce, en toute circonstance.
- La sécurité de l'information numérique est basée sur des notions de disponibilité, d'intégrité, de confidentialité, d'authentification et d'irrévocabilité.

6 ORIENTATIONS

6.1 Protection, utilisation et transmission des renseignements personnels

La Société traite de manière confidentielle tous les renseignements personnels qu’elle détient. À cette fin, à chacune des étapes de la gestion de l'information, elle prend des mesures de sécurité appropriées pour assurer la protection des renseignements confidentiels et personnels au sens de la Loi sur l'accès.

La Société limite la collecte des renseignements personnels à ceux qui sont nécessaires à l’exercice de ses attributions ou à la mise en œuvre de ses programmes.

La Société veille à ce que les renseignements personnels qu’elle détient soient exacts et à jour. De plus, elle limite leur utilisation aux fins pour lesquelles ils ont été recueillis. Elle ne les conserve que le temps nécessaire pour répondre au besoin qui avait été déterminé. La Société restreint l’accès à ces renseignements aux seules personnes qui en ont besoin dans l’exercice de leurs fonctions.

Les renseignements personnels détenus par la Société sont dans des fichiers qui font l’objet d’une déclaration obligatoire relative à la nature des renseignements, à leur pertinence et aux catégories de personnes qui y ont accès.

La Société doit prendre toutes les mesures nécessaires pour assurer la confidentialité de l’information lors de la transmission de dossiers contenant des renseignements personnels. Elle ne transmet ces renseignements qu’avec le consentement de la personne concernée ou, en l’absence d’un tel accord, lorsque la Loi sur l’accès le permet.

Toute communication de renseignements personnels sans le consentement de la personne concernée est évaluée au préalable, afin de déterminer sa conformité avec la Loi sur l'accès. Elle est également soumise pour autorisation au responsable de la PRP.

6.2 Protection de l'information et cycle de vie

L'information détenue par la Société est essentielle à sa mission et à ses activités courantes. Elle doit également être utilisée et protégée de manière adéquate durant tout son cycle de vie. Les détenteurs des actifs informationnels sont responsables de la sécurité de ces renseignements ainsi que de l'application des directives et des mesures de contrôle de la Société.

La protection de l'information dont la Société dispose s'appuie sur l'engagement formel et continu de tout le personnel ainsi que des utilisateurs à protéger l'information et le support mis à leur disposition en l'utilisant avec discernement et aux seules fins prévues. De plus, toutes les personnes concernées doivent s'engager à ne pas mettre en péril l'intégrité des actifs informationnels et à préserver le caractère confidentiel de l'information.

6.3 Sécurité d'accès

Des mesures seront mises en place pour contrôler en tout temps l'accès aux locaux de la Société et permettre d'identifier les personnes autorisées à y entrer.

L'accès au réseau local et aux systèmes d'information de la Société doit être accordé au moyen d'un logiciel de contrôle d'accès. Ce dernier doit permettre l'accès uniquement aux personnes dûment autorisées, au moyen d'un code d'identification personnel unique et authentifié par un mot de passe.

L'attribution des accès à des systèmes d'information comportant des renseignements personnels se fait après avoir déterminé quels sont les membres du personnel dont les tâches nécessitent un tel accès.

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

La Société peut adopter des directives pour assurer l'uniformité et la mise en œuvre des mesures de sécurité.

6.4 Intégrité de l'information et valeur juridique

La Société doit maintenir l'intégrité de tout document ayant une valeur juridique malgré l'interchangeabilité de son support, afin de préserver son admissibilité éventuelle devant les tribunaux.

À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et, par conséquent, de sa valeur probante.

6.5 Sensibilisation et formation

La Société doit déployer et appuyer les efforts nécessaires pour sensibiliser son personnel aux obligations et aux pratiques en matière d'accès à l'information, de PRP, de SI et de sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'à son rôle et à ses obligations dans le processus de protection de ces ressources. En conséquence, elle doit offrir à son personnel de la formation pertinente sur ces sujets ainsi que sur les procédures de sécurité existantes et l'utilisation adéquate de l'information et des technologies de l'information dont il fait usage dans l'exercice de ses fonctions. La Société doit également tenir à jour un registre de ses activités de sensibilisation et de formation en ces matières.

6.6 Destruction et archivage

Conformément à son calendrier de conservation des documents, la Société doit détruire de manière sécuritaire les actifs informationnels et les documents ne devant pas être conservés de façon permanente.

6.7 Acquisition ou développement d'applications informatiques

Les exigences en matière de PRP et de SI doivent être prises en considération dès le début des études menant à l'acquisition ou au développement d'un système d'information. Les mesures de protection requises doivent être appliquées tout au long du processus de conception.

6.8 Évaluation des risques en sécurité de l'information

Les risques et les menaces pour la sécurité de l'information doivent faire l'objet d'évaluations périodiques. Ainsi, des mesures de sécurité doivent être mises en œuvre en fonction des risques propres à l'information et selon les risques résiduels acceptables.

6.9 Respect de la propriété intellectuelle

Tous les utilisateurs doivent se conformer aux exigences légales concernant l'utilisation des produits logiciels propriétaires ainsi que des produits, des documents et de l'information qui pourraient être protégés par des droits de propriété intellectuelle.

7 RÔLES ET RESPONSABILITÉS DES DIFFÉRENTS ACTEURS

7.1 Responsable de la politique

Le président-directeur général de la Société est responsable de la présente politique. À ce titre, il s'assure du respect des lois, des règlements et des directives en matière de gestion de l'information. Il doit principalement :

- mettre sur pied un comité sur l'accès à l'information et la protection des renseignements personnels et attribuer les rôles et responsabilités prévus à la présente politique à des membres du personnel de la Société;
- établir un processus officiel de gestion intégrée et d'amélioration continue de la sécurité de l'information. À cet effet, une structure organisationnelle qui définit clairement les rôles et les responsabilités des employés de tous les échelons s'avère essentielle;
- veiller à ce que le personnel de direction ou d'encadrement de la Société soit sensibilisé aux obligations de même qu'aux pratiques en matière d'accès à l'information et de renseignements personnels, et qu'il reçoive la formation pertinente;
- instaurer un mécanisme pour définir et évaluer les risques en matière de sécurité de l'information ainsi que pour déterminer l'adéquation des mesures de sécurité en vigueur avec ces risques.

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

Le comité sur l'accès, la sécurité de l'information et la protection des renseignements personnels (CASIPRP) a la responsabilité de coordonner les activités liées à l'accès à l'information, à la PRP et à la SI au sein de la Société. Il suggère à la Société les mesures particulières de PRP qui devraient encadrer les projets d'acquisition, de développement ou de refonte d'un système d'information et de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels. Le comité doit aussi être consulté sur les mesures particulières à respecter en matière de PRP pour les sondages et la vidéosurveillance.

Présidé par le président-directeur général ou la personne qu'il désigne, ce comité est pluridisciplinaire afin de s'assurer de prendre en considération tous les aspects de la PRP et de la SI. Il est composé entre autres des personnes suivantes :

- les principaux gestionnaires qui détiennent l'actif informationnel;
- le responsable de l'accès aux documents et de la protection des renseignements personnels;
- le responsable de la sécurité de l'information (RSI);
- le responsable de la gestion documentaire (RGD).

7.3 Gestionnaire qui détient les actifs informationnels

Le gestionnaire qui détient les actifs informationnels doit faire en sorte que la PRP et la SI soient une préoccupation constante pour son personnel. Il doit sensibiliser les employés à l'importance des enjeux concernant l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information, et les informer sur ces sujets. Il doit également s'assurer que les moyens de sécurité sont employés de façon à protéger l'information que son personnel utilise. Il est le premier responsable de la sécurité et doit voir à ce que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement.

7.4 Responsable de l'accès aux documents et de la protection des renseignements personnels

Il incombe au responsable de l'accès aux documents et de la protection des renseignements personnels d'aider le personnel à mieux circonscrire l'interprétation et l'administration de la Loi sur l'accès lors de toute situation impliquant la cueillette, la communication, la conservation et la destruction de renseignements confidentiels ou personnels. Les déclarations de fichiers de renseignements personnels sont réunies dans un répertoire.

7.5 Responsable de la sécurité de l'information

La principale tâche du responsable de la sécurité de l'information (RSI) est d'assister le président-directeur général dans l'établissement d'un processus de gestion intégrée et d'amélioration continue de la sécurité de l'information détenue par la Société. Il l'aide également à déterminer les orientations stratégiques et les priorités d'intervention. De plus, il doit harmoniser l'action des divers acteurs en ce qui a trait à l'élaboration, à la mise en place, au suivi et à l'évaluation de la sécurité de l'information en général, en plus de faire connaître la *Directive sur la sécurité de l'information gouvernementale* et les exigences qu'entraîne son application. Le RSI se réserve le droit d'intervenir, au nom de la Société, lorsqu'il juge que la sécurité des actifs informationnels ou la protection des renseignements personnels sont menacées.

7.6 Responsable de la sécurité de l'information numérique

La Société peut également nommer un responsable de la sécurité de l'information numérique (RSIN). Sa principale tâche est de soutenir le RSI dans la gestion et la coordination du volet numérique de la sécurité de l'information. Il doit notamment proposer au RSI des orientations, des plans et des bilans relatifs à l'information numérique. Le RSIN travaille en étroite collaboration avec les autres acteurs en sécurité de l'information. Il se réserve le droit d'intervenir, au nom de la Société, lorsqu'il juge que la sécurité des actifs informationnels ou la protection des renseignements personnels sont menacées.

7.7 Responsable de la gestion documentaire

Le responsable de la gestion documentaire (RGD) est consulté pour la conception des systèmes de la Société et s'assure que les documents auront, à toutes les étapes de leur cycle de vie, les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois. Le RGD collabore étroitement avec le RSI dans la détermination et la mise en œuvre des mesures de sécurité de l'information. Il prépare aussi un calendrier de conservation des documents.

7.8 Répondant en éthique

Le répondant en éthique participe à l'intégration de l'éthique dans le processus de gestion de la sécurité de l'information afin, notamment, d'assurer la régularisation des conduites et la responsabilisation individuelle. Il collabore étroitement avec le RSI et le RSIN, de même qu'avec tous les autres acteurs en sécurité de l'information.

7.9 Direction des ressources humaines

La Direction des ressources humaines s'assure que tous les nouveaux employés de la Société possèdent l'information leur permettant d'assumer leurs responsabilités en matière d'accès à l'information, de PRP et de SI.

7.10 Utilisateurs

Les responsabilités des utilisateurs consistent à appliquer et à respecter les lois et règlements propres à leur domaine d'activité ainsi que toutes politiques, directives, normes, mesures et procédures établies notamment par le détenteur. Ils sont également tenus d'utiliser les moyens de sécurité et de PRP selon les modalités établies par le CASIPRP.

Les utilisateurs se doivent d'aviser leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité des actifs informationnels et des renseignements détenus par la Société.

Tout utilisateur des systèmes de la Société a l'obligation de signaler sans tarder au détenteur ou au responsable d'une unité administrative tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité, tel que le vol, l'intrusion dans un réseau ou un système, des dommages délibérés, l'utilisation abusive ou malveillante, la fraude, les actions contraires à l'éthique, etc.

7.11 Responsable des ressources informationnelles

Le rôle du responsable des ressources informationnelles (RRI) à l'égard de la sécurité consiste à fournir des conseils et des services. Elle assiste les gestionnaires et les détenteurs en leur fournissant des moyens techniques de sécurité, comme un contrôle d'accès, un plan de

sauvegarde, un plan de secours, un antivirus, etc. Le RRI s'assure de la conformité de ces moyens technologiques avec les besoins de la Société en matière de PRP et de SI. Il veille également à ce que le développement du système informatique soit adapté à l'accès à l'information, à la PRP et à la SI. Il élabore et met en œuvre les directives, les pratiques et les procédures propres à son domaine d'intervention. Il fournit les moyens et les mécanismes de sécurité permettant d'assurer la protection des actifs informationnels et la continuité des services (RSIN – Infrastructure), en plus de voir à ce que la sécurité de l'information soit intégrée dans le développement des systèmes informatiques (RSIN – Développement). Aussi, le RRI détermine les responsabilités de l'équipe de réponse aux incidents et s'assure que l'agent de liaison technique contribue efficacement au réseau d'alerte gouvernemental. Enfin, il participe à la préparation du plan d'action et du bilan de sécurité de l'information.

7.12 Coordonnateur de la cellule d'intervention et du Plan de continuité des services

Le coordonnateur de la cellule d'intervention et du Plan de continuité des services est responsable de la gestion et de la coordination du Plan de continuité des services de la Société. Il veille ainsi à la mise en œuvre et à la mise à jour du plan.

7.13 Responsable de la vérification interne

Le responsable de la vérification interne participe aux mécanismes de coordination et de concertation de la Société en matière de SI. Il exerce un rôle-conseil, notamment au regard de la définition, de l'évaluation et de la gestion des risques en matière de SI.

8 ENTRÉE EN VIGUEUR ET APPROBATION

La présente politique remplace la *Politique de protection des renseignements personnels et de la sécurité de l'information numérique* du 27 août 2002 et entre en vigueur sur approbation du conseil d'administration de la Société du 5 février 2010.

ANNEXE 1 : LOIS, RÈGLEMENTS ET DIRECTIVES

La présente liste comprend les lois, règlements et directives dont la Société doit tenir compte dans le cadre de la mise en œuvre des mesures destinées à assurer la sécurité de l'information et la protection des renseignements personnels.

- *Charte canadienne des droits et libertés*, partie 1 de la *Loi constitutionnelle de 1982* [annexe B de la *Loi de 1982 sur le Canada* (1982, R.-U., c. 11)], art. 5 et 44.
- *Charte des droits et libertés de la personne, L.R.Q., c. C-12*.
- *Code civil du Québec, L.Q. 1991, c. 64*, art. 35 à 41.
- *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*, en ce qui a trait aux exigences relatives à la protection et à la conservation des documents électroniques ayant une valeur patrimoniale ou archivistique.
- *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. C-42*.
- *Loi sur la fonction publique, L.R.Q., c. F-3.1.1*.
- *Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1*.
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, (2008) 140 G.O. II, 2081*.
- *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels, (1993) 125 G.O. II, 97*.
- *Règlement sur les organismes publics tenus de refuser de confirmer l'existence et de donner communication de certains renseignements, (1994) 126 G.O. II, 3982*.
- *Règlement sur l'éthique et la discipline dans la fonction publique, (2002) 134 G.O. II, 7639*.
- *Directive sur la sécurité de l'information gouvernementale*, 11 avril 2006, entrée en vigueur le 1er mai 2006.
- *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 un support informatique amovible*, 27 mai 2003.
- *Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique*, 1er octobre 2002.

- *Directive sur la gestion des ressources informationnelles*, 18 juin 2007.
- *Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'administration publique*, 13 juin 2006.
- *Règles de preuve et de procédure de la Commission d'accès à l'information, (1984) 116 G.O. II, 4648.*
- Modèle de gestion de la sécurité de l'information gouvernementale, version 1.0, mars 2009.
- *Guide de référence : Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, mai 2008.
- *Guide de destruction sécuritaire de l'information, pratique recommandée (*PR-55), version 1.0, janvier 2009.

ANNEXE 2 : LEXIQUE

« Actifs informationnels » : ensemble de l'information inscrite sur un support papier ou électronique, des logiciels, de l'équipement informatique, des banques d'information numérique et des systèmes d'information qui les supportent que la Société a acquis, développés ou constitués et qui fait appel aux technologies de l'information.

« Application informatique » : logiciel conçu pour répondre à un ensemble de besoins dans un domaine d'application donné.

« Authentification » : acte permettant de vérifier l'identité d'une personne ou la validité d'un dispositif.

« Calendrier de conservation » : liste des règles de conservation et d'élimination déterminées pour l'ensemble des séries documentaires d'une organisation.

« Confidentialité » : propriété d'une information de n'être accessible qu'aux personnes autorisées.

« Détenteur » : personne responsable de la sécurité d'un système d'information.

« Disponibilité » : propriété d'une information d'être accessible en temps voulu et de manière requise par une personne autorisée.

« Fichiers de renseignements personnels » : collection de renseignements personnels organisée selon des modalités fixées par l'organisme dans le cadre de ses mandats.

« Fournisseur » : personne morale, société, coopérative ou personne physique qui exploite une entreprise individuelle, à l'exception d'un organisme public.

« Gestionnaire » : fonctionnaire d'un échelon supérieur ou en situation de gestion chargé, dans les limites d'un mandat qui lui est confié, de la gestion des crédits budgétaires, de l'élaboration des prévisions budgétaires, de l'affectation du personnel, de l'organisation matérielle et d'autres fonctions de niveau supérieur en rapport avec l'administration gouvernementale.

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

« Informations stratégiques » : renseignements dont la divulgation aurait vraisemblablement des incidences néfastes pour la Société ou un tiers, par exemple : un avis, une recommandation ou une analyse remis à la Société; un examen utilisé lors d'un concours et sa grille d'analyse; une opinion juridique; un projet de texte législatif ou réglementaire; un brouillon, une ébauche ou des notes personnelles; certains détails d'une soumission; des renseignements de nature commerciale, financière, industrielle, technique, syndicale ou scientifique.

« Irrévocabilité » : propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

« Intégrité » : propriété d'une information ou d'une technologie de l'information de ne pouvoir être ni modifiée ni détruite sans autorisation.

« Partenaires » : organisme public ou privé avec lequel la Société partage des actifs informationnels.

« Renseignements confidentiels » : renseignements qui englobent les renseignements personnels et les renseignements stratégiques.

« Renseignements personnels » : renseignements qui concernent une personne physique et qui permettent de l'identifier, par exemple : un nom, une adresse, une photographie, un numéro d'assurance sociale, des renseignements financiers (dossier fiscal, revenu, bilan financier, renseignements bancaires, cartes de crédit, etc.), des renseignements sur l'identité d'une personne qui porte plainte ou dénonce une autre personne, l'origine ethnique, la religion, l'expérience de travail et la scolarité, l'état de santé physique ou mentale.

« Système d'information » : ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y compris notamment les technologies de l'information et les procédés aménagés pour accomplir ces fonctions.

« Télécommunication » : ensemble de procédés électroniques de transmission d'information à distance.

« Utilisateur » : toute personne qui, dans les locaux de la Société ou à distance, utilise les technologies de l'information et les actifs informationnels de la Société.