POLITIQUE SUR LA GESTION ET LA SÉCURITÉ DE L'INFORMATION

Service de la technologie
2016

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Préface

Groupe Ultima inc. (« Ultima ») reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate.

Ultima reconnaît également détenir ou avoir accès à des renseignements personnels, ainsi que des informations sensibles, pouvant avoir une valeur légale, administrative ou économique.

En conséquence, Ultima met en place la présente politique concernant la gestion et la sécurité de l'information qui exprime la prise de position de l'organisation concernant les mécanismes de sécurité considérés comme essentiels à la protection des ressources (i.e. actifs) informationnelles.

Une gestion et une sécurité fiable et efficace s'appuient sur l'implication continue et le support de tous les employés et individus ayant un lien contractuel avec Ultima utilisant des informations de l'entreprise dans le cadre de leurs fonctions. Ces derniers sont responsables de la gestion de l'information dont ils ont le contrôle et la garde, du respect des présentes normes et politiques.

1.2 Objectifs

Compte tenu qu'Ultima reçoit, utilise et transmet bon nombre d'informations, étant donné la nature de ses services, la mise en place d'une politique globale de gestion et de sécurité de l'information s'avère nécessaire. L'objectif de cette politique est d'établir un cadre formel régissant l'utilisation des équipements informatiques et des informations à travers le réseau technologique (informatique et télécommunications) d'Ultima en partant du poste de travail jusqu'aux serveurs. Plus particulièrement, l'objectif principal de la présente politique est de garantir que l'information dont Ultima a le contrôle est gérée et sécurisée de façon efficace et efficiente, afin d'éviter de compromettre sa crédibilité et sa conformité.

La présente politique vise également à assurer le respect des lois, règlements et autres à l'égard de l'utilisation de l'information et des technologies de l'information.

Quant à la sécurité de l'information, plus spécifiquement, les objectifs de l'organisation sont :

- D'assurer la disponibilité, l'intégrité et la confidentialité à l'égard de l'utilisation des actifs informationnels et des réseaux informatiques;
- D'assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère nominatif relatifs aux clients et au personnel de l'organisation;
- De regrouper les lignes directrices et les rôles et responsabilités des intervenants en sécurité.

Cette politique comprendra une série de directives, procédures, standards ou pratiques, afin de préciser les modalités et les obligations découlant de celle-ci afin de mettre en place un mécanisme de gestion et de sécurité de l'information.

1.3 Portée

La présente politique s'applique aux :

Actifs informationnels (voir lexique)

- Ceux appartenant à l'organisation et exploités par elle-même;
- Ceux appartenant à l'organisation et exploités ou détenus par un fournisseur de services;
- Ceux appartenant à un tiers.

Personnel de l'organisation : Tout le personnel de l'organisation, régulier ou occasionnel, peu importe son statut, ainsi qu'à toute personne dûment autorisée qui a recours à l'actif informationnel de l'organisation. Les consultants utilisant et ayant accès aux biens de l'organisation ou ayant des biens de l'organisation sous leur garde ont les mêmes obligations que le personnel de l'organisation.

Activités : Toutes les activités impliquant la manipulation ou l'utilisation sous toutes ses formes des actifs informationnels de l'organisation, que celles-ci soient conduites dans ses locaux, dans un autre lieu ou à distance.

2. CADRE LÉGAL

Plusieurs lois, règlements, directives encadrent et régissent l'utilisation de l'information.

L'organisation est assujettie à ces lois et doit s'assurer de les respecter. Une énumération sommaire est présentée :

- *Charte canadienne des droits et libertés* (1982, c. 11)
- *Charte des droits et libertés de la personne* (L. R.Q., c. C-12)
- *Code civil du Québec* (L.Q., 1991 c. 64)
- *Code criminel du Canada*
- *Loi canadienne sur le droit d'auteur* (L. R., c. C-42)
- *Loi concernant le cadre juridique des technologies de l'information*
- *Loi sur la distribution de produits et services financiers (L.R.Q., D-9.2)*
- *Loi sur la propriété intellectuelle et les marques de commerce* (L.R. 1985, c. T-13)
- *Loi sur la protection des renseignements personnels et les documents technologiques (Loi fédérale)*
- *Loi sur la protection des renseignements personnels dans le secteur privé*
- *Loi sur les archives* (L.R.Q., c. A-21.1)
- *Loi sur les assurances (L.R.Q., c. A-32)*
- *Loi sur les sociétés d'assurances (L.Q. 1991, c. 47)*

3. PRINCIPES DIRECTEURS

3.1 Gestion et protection des actifs informationnels

Les actifs informationnels de l'organisation sont essentiels à ses opérations courantes et doivent faire l'objet d'une utilisation et d'une protection adéquate. Cette politique globale de gestion et de sécurité de l'information est fondée sur les lignes directrices suivantes :

Gestion des actifs informationnels

a. L'information contenue dans les actifs informationnels est présumée de nature confidentielle;

b. Les actifs informationnels sont gérés afin d'en faciliter l'accès légal, de favoriser la confiance des clients et partenaires, d'optimiser l'utilisation de l'information conformément aux obligations imposées par les lois et règlements;

c. La collecte, l'utilisation et la communication des renseignements personnels doit être restreinte aux minimum nécessaire pour assurer la prestation de services, conformément à la Loi sur la protection des renseignements personnels ou autres lois en vigueur. De plus, l'information créée, acquise ou conservée pour répondre aux besoins doit être pertinente, fiable et complète;

d. La collecte, l'utilisation et la communication des informations, peu importe sa forme ou le support sur lequel elle est enregistrée, doit être réalisée d'une manière qui en protégera l'authenticité, l'intégrité et la clarté aussi longtemps que nécessaire;

e. Des structures de responsabilisation doivent être mises en place. Quant au niveau de protection, il est accordé en fonction de la sensibilité des actifs informationnels et des risques d'accidents, d'erreurs et de malveillance auxquels ils sont exposés;

f. Les gestionnaires, particulièrement ceux qui sont désignés comme propriétaires/détenteurs d'actifs informationnels, sont les premiers responsables de la gestion de ces actifs, de leur utilisation par les employés et de l'application des mesures de contrôle nécessaires;

g. L'utilisation des actifs informationnels est un privilège et non un droit. Ce privilège peut être retiré en tout temps. Tout usager qui ne se conforme pas à la politique globale de gestion et de sécurité de l'information, incluant ses directives peut se voir révoquer ce privilège.

Protection des actifs informationnels

h. Une évaluation périodique des risques, des menaces et des mesures de protection des actifs informationnels doit être effectuée, afin d'obtenir l'assurance qu'il y a adéquation entre les risques, les menaces et les mesures de protection déployées;

i. Les documents essentiels à la continuité des services et des opérations clés doivent être protégés;

j. L'information, qui n'est plus requise à des fins opérationnelles, doit être éliminée de façon opportune;

k. La gestion de la sécurité de l'information doit être incluse et appliquée tout au long du cycle de vie d'un actif informationnel;

l. Personne ne peut modifier ou détruire les données, logiciels, progiciels, documentation, systèmes d'information et les équipements informatiques ou de télécommunication sans autorisation.

3.2 Signalement des incidents

Tout utilisateur a l'obligation de signaler sans tarder au responsable de l'Administration toute irrégularité ou contravention à la présente politique ou tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que vol, intrusion dans un réseau ou système, dommages délibérés, utilisation abusive, fraude, divulgation d'informations, etc.

3.3 Droits de propriété intellectuelle ou de droit

Les utilisateurs doivent se conformer aux exigences légales sur l'utilisation de produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle et sur l'utilisation de produits logiciels propriétaires. Toutes reproductions de logiciels ne sont autorisées qu'à des fins de copies de sécurité.

3.4 Protection des renseignements confidentiels

Toute information électronique ou non considérée confidentielle ou sensible doit être protégée contre tout accès ou utilisation non autorisés ou illicites. Sont notamment confidentiels au sens de la Loi sur la protection des renseignements personnels, les renseignements nominatifs ainsi que tout renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

3.5 Continuité des activités de l'organisation

L'organisation doit disposer de mesures d'urgence issues de son plan de continuité et de relève des services, consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise en opération dans un délai raisonnable des actifs informationnels jugés essentiels en cas de sinistre majeur.

3.6 Sensibilisation et formation

Chaque gestionnaire de l'organisation doit sensibiliser son personnel à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'au rôle et obligations de tous les employés dans le processus de protection de ses actifs. Il doit également veiller à ce que le personnel soit formé sur les procédures de sécurité et sur l'utilisation correcte des actifs informationnels afin de minimiser les risques de sécurité possibles.

3.7 Droit de regard

L'organisation a un droit de regard sur l'utilisation de ses actifs informationnels par les utilisateurs, notamment l'Internet, les systèmes de téléphonie et de courrier électronique. Les circonstances pour lesquelles ce droit de regard peut être exercé seront définies et diffusées auprès des utilisateurs dans les directives découlant de la politique. Ce droit de regard sera exercé conformément à la législation notamment la Charte canadienne des droits et libertés (L.R.C. (1985) c-42) et la Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12).

4. RESPONSABILISATION POUR LA POLITIQUE

Le comité de direction d'Ultima doit approuver la présente politique, assurer sa mise en œuvre et le suivi de son application au sein des fonctions corporatives. Il met en place le C*omité sur la gestion et la sécurité de l'information* qui agit à titre de mécanisme de coordination et de concertation au sein de l'organisation. Ce comité nomme le responsable de l'application de la politique globale et le responsable de la sécurité de l'information. De plus, il recommande les orientations et les directives au comité de direction.

4.1 Le responsable de l'Administration, finances et ressources humaines

L'application de la politique globale de gestion et de sécurité de l'information relève de la vice-présidence Administration, finances et ressources humaines.

Elle doit s'assurer que les valeurs et les orientations en matière de sécurité sont partagées par l'ensemble des gestionnaires et du personnel de l'organisation.

À cette fin, elle s'assure de l'application de la politique dans l'organisation, apporte les appuis financiers et la logistique nécessaire pour la mise en œuvre et l'application de la présente politique, soumet un compte-rendu sommaire concernant l'application de la politique au conseil d'administration, exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

4.2 Le responsable de la Sécurité de l'information

La réalisation de l'ensemble des mesures liées à la sécurité de l'information relève de la vice-présidence, Technologie. Elle agit comme responsable désignée pour coordonner la sécurité de l'information de l'organisation. À cet effet, elle a la responsabilité :

- de proposer les orientations de sécurité de l'information et les communiquer au personnel, aux clients et partenaires de l'organisation;
- d'élaborer et d'assurer le suivi et la mise à jour périodique des politiques de sécurité de l'information;
- de veiller au respect de la politique de sécurité de l'information;
- de s'informer des besoins en matière de sécurité auprès des détenteurs et des gestionnaires, de leur proposer des solutions et de coordonner la mise en place de ces solutions;
- de fournir aux détenteurs d'actifs informationnels le soutien et les conseils en matière de sécurité;

- de proposer les standards, directives ou procédures découlant de la mise en œuvre de la présente politique;
- de gérer les aspects relatifs à l'escalade des incidents de sécurité et procéder à l'évaluation de la situation en matière de sécurité.

4.3 Le responsable de l'informatique

La mise en application des exigences en matière de sécurité des actifs informationnels de l'organisation relève du vice-président, Technologie. Le responsable de l'informatique assure la mise en application des exigences de sécurité des actifs informationnels de l'organisation. Ses principales responsabilités sont de :

- assurer la sécurité des actifs informationnels;
- assurer la disponibilité, l'intégrité, la confidentialité selon les exigences définies par les détenteurs des actifs informationnels;
- restreindre les accès de son personnel spécialisé en technologies de l'information aux seules informations indispensables à l'exercice de leurs fonctions;
- superviser l'application des directives, pratiques et standards.

5. DISPOSITIONS FINALES

5.1 Mesures en cas de non-respect de la politique

Toute violation ou non-respect de cette politique globale de gestion et de sécurité de l'information pourra donner lieu à des mesures administratives et/ou disciplinaires, notamment un avis, une réprimande, une suspension ou même un congédiement immédiat, selon les circonstances, lesquelles mesures seront proportionnelles au comportement en question. Il incombera aux responsables de fonctions corporatives, conjointement avec les responsables de l'administration, de décider des mesures appropriées à prendre en cas de violation ou de non-respect de cette politique.

Le comité de direction pourra aussi référer aux autorités compétentes toute information qui pourra le porter à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

5.2 Examen et révision

La présente politique fera l'objet de révisions périodiques par le comité sur la gestion et la sécurité de l'information. Elle pourra aussi être modifiée au besoin afin de la rendre conforme aux dispositions législatives et/ou réglementaires pertinentes ou de refléter de nouvelles pratiques ou méthodes d'opération de la Compagnie. Les salariés seront avisés en temps opportun de toute modification.

5.3 Date d'entrée en vigueur

La présente politique globale sur la gestion et la sécurité de l'information est en vigueur depuis le 15 janvier 2008.

6. LEXIQUE

Actif informationnel : Une information numérique, une banque d'information numérique, un système ou un support d'information, une documentation, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par une organisation.

Application : 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 : Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

Autorisation : Attribution par une autorité de droits d'accès aux actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité.

Banque d'information : Collection d'information relative à un domaine défini, regroupée et organisée de façon à en permettre l'accès.

Confidentialité : Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et 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.

Destruction de l'information : Action de faire disparaître l'information.

Détenteur : Gestionnaire à qui est assignée la responsabilité de la sécurité d'un actif informationnel et/ou d'un processus d'affaires.

Directives : Énoncés particuliers qui viennent en appui à la politique globale et permettent de la développer et de la préciser en déterminant les mécanismes concrets et la façon de procéder en vue d'assurer la sécurité des actifs informationnels.

Droit d'auteur : Droit exclusif que détient un auteur ou son représentant d'exploiter une œuvre pendant une durée déterminée.

Équipement informatique : Ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunications.

Fournisseur : Corporation, société, coopérative ou personne physique faisant affaires et étant en mesure de contracter avec l'organisation qui fournit des services ou des biens à un détenteur, à un utilisateur ou à un autre fournisseur.

Incident de sécurité : Circonstance au cours de laquelle la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel a été affectée de même que toute situation présentant les conditions requises pour potentiellement produire un tel résultat.

Information : Élément de connaissance concernant un phénomène et qui, pris dans un contexte déterminé, a une signification particulière.

Information électronique : Information sous toute forme (textuelle, symbolique, sonore ou visuelle) dont l'accès et l'utilisation ne sont possibles qu'au moyen des technologies de l'information.

Intégrité : Propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

Logiciel : Ensemble des programmes, des procédures et des règles, ainsi que de la documentation qui leur est associée, nécessaires à la mise en œuvre d'un système de traitement de l'information.

Mécanisme de sécurité : Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

Mot de passe : Authentifiant prenant la forme d'une chaîne de caractères alphanumériques, généralement choisie par l'utilisateur, que celui-ci doit entrer lors de la procédure d'accès à un système informatique, notamment à un réseau ou à sa boîte aux lettres électronique.

Norme : Accord documenté contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi. Le terme « norme » accompagné du qualificatif « internationale », « nationale » ou « européenne » signifie une norme reconnue par un organisme officiel.

Politique de gestion et de sécurité de l'information : Ensemble de documents produits constitués de la politique globale, des directives, des standards, des pratiques et des procédures qui régissent les exigences d'une organisation en matière de gestion et de sécurité de l'information.

Pratique : Savoir ou manière de faire qui, dans une organisation, conduisent au résultat souhaité et qui sont portés en exemple auprès des pairs afin de leur faire partager l'expérience qui leur permettra une amélioration collective.

Procédure : Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.

Personne : Une personne physique ou une personne morale de droit public ou de droit privé.
Personnel : Ensemble des ressources humaines, rémunérées ou non, qui assument la mission de l'organisme.

Renseignement personnel ou nominatif : Information de caractère non public concernant une personne physique et permettant de l'identifier, directement ou indirectement.

Réseau : Ensemble d'équipements qui sont reliés les uns aux autres par des câbles ou des faisceaux hertziens, afin qu'ils puissent échanger, distribuer ou diffuser des informations et partager différentes ressources.

Ressources informationnelles : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Sécurité de l'information : Protection des ressources informationnelles d'une organisation, face à des risques identifiés, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée.

Standard : Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation comme l'ISO, le CCN[1], etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'organisations ou encore d'un consortium.

Système d'information : Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents au fonctionnement d'une entreprise ou d'une organisation.

Utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé ayant accès à l'actif informationnel, ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, accède à l'actif informationnel de l'organisation.

Utilisation : Terme qui recouvre, le cas échéant, l'ensemble des événements constituant le cycle de vie de l'information électronique dont, entre autres, la création, la collecte, le traitement, la conservation, l'interrogation, la communication, la modification, l'archivage et la destruction.

[1] CCN : Conseil canadien des normes