POLITIQUE DE SÉCURITÉ DE L'INFORMATION

1. PRÉAMBULE

Guide Succession Inc. reconnait que l'information est essentielle à ses opérations courantes et qu'elle doit donc faire l'objet d'une utilisation appropriée et d'une protection adéquate. L'entreprise reconnait détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur légale ou administrative. Plusieurs lois et directives encadrent et régissent l'utilisation de l'information. Guide Succession Inc. est assujettie à ces lois et doit s'assurer du respect de celles-ci.

Dans la présente politique, la sécurité de l'information se définit comme étant l'ensemble des mesures adoptées pour éviter l'utilisation non-autorisée, le mauvais usage, la modification ou le refus d'utilisation d'un ensemble de données. Le terme sécurité de l'information désigne donc les mesures préventives que Guide Succession met en place pour préserver l'information.

1.1. Objectifs de la politique

La présente politique vise à assurer le respect par Guide Succession Inc. de toute obligation opérationnelle et de toute législation à l'égard de l'usage et du traitement de l'information, autant les actifs informationnelles que les échanges électroniques.

Plus spécifiquement, les objectifs de Guide Succession en matière de sécurité de l'information sont :

a) D'identifier, de réduire et de contrôler les risques pouvant porter atteintes aux informations ou aux système d'informations de Guide Succession ou de ses clients.

b) D'assurer l'intégrité, l'irrévocabilité, la disponibilité, la confidentialité, le contrôle d'accès, la surveillance et l'administration à l'égard de l'utilisation des réseaux informatiques, des télécommunications et d'internet, de l'utilisation des actifs informationnels et des données corporatives; d'assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements

c) D'assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs à la clientèle, au personnel de Guide Succession à tout partenaire d'affaires de Guide Succession provenant du milieu des affaires ou de l'industrie;

d) D'assurer la conformité aux lois, aux règlements applicables et aux exigences de la Chambre des Notaires de Québec;

e) D'établir un plan de continuité et de relève des services informatiques de Guide Succession.

f) La présente politique fait référence à la Directive de sécurité, les ententes de confidentialité, les contrats avec les sous-traitant et le contrat d'utilisation du logiciel qui supportent tous la politique.

1.2. Respect de la politique

Le conseil d'administration est responsable de l'application de la présente politique.

Le conseil d'administration de Guide Succession entend bien insister sur l'importance de la sécurité de l'information pour l'avenir de Guide Succession et l'obligation de se conformer aux exigences de la présente politique.

Par conséquent, l'entreprise exige de toute personne, qui utilise les actifs informationnels de Guide Succession ou qui a/aura accès à de l'information, de se conformer aux dispositions de la présente politique ainsi qu'aux directives, procédures et standards qui s'y rattachent.

La Directive de la Chambre des notaires s'applique aux tiers concernés et ils doivent s'y conformer. Par conséquent, si Guide Succession sous-traite en totalité ou en partie ses services, Guide Succession s'assure que le sous-traitant respecte en tout point la Directive et que celui-ci signe une entente à cet effet. Guide Succession déclare et fournit une preuve que l'entente de sous-traitance est conforme aux engagements pris par le fournisseur avec la Chambre des notaires et avec ses clients notaires. Guide Succession n'est pas propriétaire des infrastructures seront traitées les données notariales.

1.3. Portée / Champ d'application

La présente politique en matière de sécurité de l'information ainsi que les directives et procédures sous-jacentes et les règles qui leur sont associées s'appliquent aux personnes, actifs et activités suivants :

a) **Personnes visées** : Cette politique s'adresse à tous les utilisateurs, cadres et tout le personnel œuvrant à Guide Succession sans égard à son statut. De plus, elle s'étend à toute personne dûment autorisée qui utilise ou qui accède dans l'exercice de ses fonctions pour le compte de Guide Succession, à des informations confidentielles ou non. Les consultants, partenaires et fournisseurs utilisant et ayant accès aux biens de Guide Succession ou ayant des biens de Guide Succession sous leur garde, ont les mêmes obligations que le personnel de Guide Succession;

b) **Actifs visés** : Cette politique s'applique à l'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein de Guide Succession, tels que les bases de données sans égard aux médiums de support (fixe ou portable), les réseaux, les systèmes d'information, les logiciels, les équipements informatiques utilisés par Guide Succession, que ces actifs fassent partie de l'une ou l'autre des trois catégories suivantes :

- ✓ appartenant à Guide Succession et exploités par cette entreprise;
- ✓ appartenant à Guide Succession et exploités ou détenus par un fournisseur de services ou un tiers.
- ✓ appartenant à un fournisseur de services ou un tiers et exploités par celui-ci au profit de Guide Succession. Dans ce cas-ci, le fournisseur doit respecter l'esprit de la présente politique.

2. CADRE LÉGAL ET ADMINISTRATIF

2.1. Les principales lois et directives servant de guides et de références à la politique de sécurité de l'information sont :

a) Les lois canadiennes et québécoises en vigueur ainsi que les règlements, politiques et directives de Guide Succession et les différentes directives de la Chambre des Notaires du Québec;

2.2. Guide Succession s'engage à respecter les dispositions législatives relativement aux différentes lois et directives ci-avant mentionnées.

3. PRINCIPES DIRECTEURS

3.1. Généralités

Cette politique de sécurité de l'information est fondée sur les énoncés généraux suivants :

a) Les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la confidentialité, l'intégrité, la disponibilité, l'accessibilité et l'irrévocabilité des actifs informationnels de même que la continuité des activités. Elles doivent notamment empêcher les accidents, les manipulations erronées ou malveillantes ou la destruction d'information sans autorisation;

b) Une évaluation périodique des risques et des mesures de protection des actifs informationnels doit être effectuée;

c) La gestion de la sécurité de l'information doit être incluse et appliquée tout au long du processus menant à l'acquisition, au développement, à l'utilisation, au remplacement ou à la destruction d'un actif informationnel par ou pour Guide Succession;

d) Les ententes et contrats dont Guide Succession est partie prenante doivent contenir des dispositions écrites garantissant le respect, par toutes les parties, des exigences en matière de sécurité et de protection de l'information. À cet effet, Guide Succession s'engage à communiquer, publier, et à faire endosser par tous ses employés

3.2. Protection des actifs informationnels

Plus spécifiquement, cette politique de sécurité de l'information est fondée sur les obligations suivantes en matière de protection des actifs informationnels :

3.2.1. Classification

Les actifs informationnels doivent faire l'objet d'une identification et d'une classification. Le niveau de protection de chaque actif informationnel doit être identifié par son détenteur en fonction de sa criticité, de sa sensibilité et des risques d'accidents, d'erreurs et de malveillance auxquels il est exposé. Afin de maintenir la protection des actifs informationnels, chaque actif sera répertorié et assigné à un propriétaire qui aura la responsabilité de maintenir les contrôles appropriés afin d'en assurer la protection.

Les données seront classifiées en termes de confidentialité et de disponibilité. Un système de classification est mis en place et toutes les données faisant l'objet du service d'externalisation seront classifiées selon le plus haut niveau dans l'échelle. Toutefois, ces données seront toutes protégées avec le plus haute niveau sécurité de l'information peut importe leur niveau de classification.

3.2.2. Protection des locaux et du matériel

a) Tous les accès physiques à des locaux comportant des actifs informationnels appartenant à Guide Succession doivent être contrôlés afin d'empêcher tout dommage ou toute intrusion. Des équipements appropriés de contrôle d'accès doivent être mis en place à l'entrée de ces locaux en fonction des risques identifiés.

b) Tout support d'informations appartenant à Guide Succession et devant être déplacé hors des locaux sécurisés doit faire l'objet d'une surveillance continue et de mesures de contrôle appropriées selon son degré de criticité afin de le préserver de tout dommage.

c) Personne ne doit détruire sans autorisation le matériel appartenant à Guide Succession. Tout dommage doit être rapporté et expliqué au détenteur de l'actif concerné. On ne peut disposer d'un actif sans avoir d'abord prévu une méthode de recyclage ou de mise au rebut sécurisé.

3.2.3. Utilisation des informations et des installations reliées

Les droits et les privilèges doivent être alloués selon le profil d'utilisation.

Les actifs informationnels doivent être protégés et utilisés avec discernement et aux seules fins prévues, de la sécurité, de l'intégralité de l'information et des traitements effectués sur les équipements.

a) Personne ne doit modifier ou détruire sans autorisation les actifs informationnels de Guide Succession.

b) Seules les personnes dûment autorisées peuvent utiliser les actifs informationnels de Guide Succession.

c) Les données seront entreposées à l'extérieur des locaux, mais en territoire canadien, une fois par semaine, dans des locaux répondant aux exigences de sécurité décrites à la directive.

d) Les archivages et les sauvegardes, peu importe le support, feront l'objet d'une procédure claire quant à leur identification et manipulation. Cette information est considérée important et confidentielle et ne sera manipulée, détenue et/ou détruite que par le personnel ou les parties autorisées.

3.2.4. Gestion de l'accès utilisateur

Une procédure d'enregistrement et de révocation des droits d'accès des comptes utilisateurs doit être en place et revue annuellement. Cette procédure doit respecter les points suivants:

a) Un identifiant unique pour chaque utilisateur.
a) Maintenir à jour une liste des utilisateurs.
b) Seulement les privilèges nécessaires doivent être associés au compte de l'utilisateur ou de l'administrateur.

Une procédure de contrôle d'accès doit être mise en place et doit respecter les points suivants :

a) Vérification de l'identité de l'utilisateur avant de lui donner un nouveau mot de passe, que ce soit temporaire ou pour un remplacement.
b) Les mots de passe temporaires doivent être transmis d'une manière sécuritaire.
c) Les mots de passe doivent respecter les meilleures pratiques au niveau de la complexité, de la fréquence de changement et l'historique :
    a. Utiliser un mot de passe d'au moins 8 caractères, composé de lettres, chiffres, d'au moins un caractère spécial (#1$%&), d'une minuscule et d'une majuscule.
    b. Éviter d'utiliser un mot de dictionnaire ou un mot qui ressemble au nom du
d) Fournisseur, du service, du logiciel, du système ou de l'employé.
e) Le verrouillage (temporaire ou permanent) des comptes doit être activé après un nombre défini de tentatives infructueuses.
f) Un système doit engendrer une déconnexion automatique des sessions inactives après un délai défini.
g) L'accès aux serveurs et aux équipements réseau doit être contrôlé au minimum par un identifiant et un mot de passe.
h) Les utilisateurs seront avisé de ne pas afficher ou écrire le mot de passe sur un papier à la vue d'autres personnes
i) Les identifiants génériques ne doivent être utilisés que lorsqu'il n'y a aucune alternative.
j) Ne pas permettre à un utilisateur d'ouvrir une session de travail sous l'identifiant d'un autre utilisateur, à moins d'avoir été formellement autorisé par le supérieur de ce dernier. Dans ce dernier cas, cette action doit être enregistrée dans un registre.
k) L'écran de veille avec mot de passe doit être activé, permettant de verrouiller automatiquement le poste de travail ou le serveur lorsqu'il est hors d'usage pendant une période maximale de dix (10) minutes ou permettant de verrouiller l'ordinateur manuellement.
l) Révoquer immédiatement les droits d'utilisation d'un administrateur lors d'un départ ou d'un Incident lié à la sécurité de l'information où sa responsabilité est en cause.
m) En aucun cas utiliser le même mot de passe à plusieurs fins.
n) Activer le verrouillage (temporaire ou permanent) des comptes après un nombre défini de tentatives infructueuses.

3.2.5. La sécurité liées aux ressources humaines

Les utilisateurs, employés de Guide Succession, doivent:

a) Utiliser les systèmes en respect des règles et politiques en vigueur.

b) Ne jamais laisser sans surveillance des Documents technologiques qui ne sont pas protégés (ex. : sans chiffrement), quel que soit le support ou le média sur lequel ils se trouvent.

c) Les démarches à suivre concernant le recrutement, l'embauche et la fin de contrat d'embauche se retrouve dans Les Directives de Sécurité de Guide Succession.

3.2.6. Systèmes d'information, serveurs et réseaux locaux

Tout système d'information doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'utilisateur. Il doit, en plus, limiter cet accès aux personnes autorisées seulement, en fonction de la nature de l'information et des applications utilisées.

a) Le départ, transfert, mutation ou autre évènement concernant les tâches et fonctions d'un utilisateur doit conduire systématiquement à la révision et à la suppression, s'il y a lieu, de tous ses accès au système d'information.

b) Guide Succession doit conserver les journaux d'accès, d'évènements de sécurité et d'activités sur les données pour une période d'au moins 12 mois. Ils doivent être analysés régulièrement afin de détecter toute anomalie sur les équipements permettant d'offrir le service d'externalisation.

c) Un plan de continuité et de relève des services informatiques de Guide Succession doit être mis en place et faire l'objet de tests de simulation périodiques en tout ou en partie. Tous les changements seront préalablement testés et approuvés dans un environnement distinct avant d'être amené vers un environnement de production.

d) Toutes le données des clients notaires demeurent en tout temps au Canada. En aucun cas, les données ne seront transitées, sauvegardées ou traitées à l'extérieur du Canada. Guide Succession s'assure que cette obligation est respectée en tout temps.

e) Guide Succession s'assure d'individualiser les données notariales de chacun de ses clients notaires sur les serveurs afin d'en protéger la confidentialité, d'en facilité la recherche et la récupération lorsque requis.

f) Guide Succession s'assure que les infrastructures permettant d'offrir le service d'externalisation sont logiquement isolées de tous les autres services.

3.2.7. Protection des applications et des processus d'exploitation

a) Le principe du « droit d'accès minimal » doit être appliqué en tout temps lors de l'attribution d'accès aux actifs informationnels. Des droits d'accès limités doivent être attribués aux personnels autorisés en fonction de ce qui lui est strictement nécessaire pour l'exécution de ses tâches.

b) La maintenance de toute application ou processus ne doit être confiée qu'à un personnel dûment habilité et autorisé.

c) Tous les changements doivent être préalablement testés et approuvés avant d'être portés sur l'environnement de la production.

d) L'environnement servant à effectuer la maintenance des applications et des processus reliés doit être isolé de l'environnement réel de production.

e) L'acquisition, le développement et la maintenance des applications doivent être règlementés et contrôlés pour éviter la possibilité d'insertion, intentionnelle ou non, de code malveillant.

f) Les applications ou processus d'exploitation susceptibles d'occasionner des répercussions sur l'information critique de Guide Succession ne doivent être accessibles que par l'intermédiaire de moyens sécurisés dans un environnement contrôlé et restreint.

g) Toute application (la documentation reliée, les logiciels utilisés et les processus nécessaires à son exécution) doit faire l'objet d'une sauvegarde appropriée pour répondre aux critères de disponibilité, d'intégrité et de confidentialité déterminés par son détenteur d'actifs.

h) Toute opération critique effectuée sur ou par l'intermédiaire d'une application ou d'un processus d'exploitation doit pouvoir être retracée par le personnel dûment habilité à l'aide de journaux d'évènements correctement sécurisés et préservés pour références futures.

i) Les ententes et contrats dont Guide Succession fait partie pour l'acquisition, le développement et la maintenance des applications doivent contenir des dispositions garantissant le respect des standards de sécurité de l'information de Guide Succession.

j) Tous les membres du personnel ayant accès aux systèmes et aux données seront authentifiés par nom d'utilisateur et mot de passe passant par un accès VPN.

3.2.8. Protection des renseignements confidentiels et stratégiques

a) Toute information considérée confidentielle ou stratégique doit être protégée contre tout accès ou utilisation non autorisés ou illicites.

b) Sont notamment jugés confidentiels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements nominatifs, les renseignements relatifs à la vie privée de la personne au sens du Code civil du Québec 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.

c) L'attribution à un fournisseur de service d'un accès à des données stratégiques doit être précédée d'un engagement formel de ce fournisseur au respect des règles élémentaires de protection des moyens d'accès fournis et du devoir de signalement en cas de divulgation non autorisée (ou même de suspicion de divulgation d'information stratégique).

d) Les renseignements personnels ne doivent être utilisés et ne servir qu'aux fins pour lesquelles ils ont été recueillis ou obtenus.

e) Guide Succession ne peut transmettre de renseignements personnels sans le consentement des personnes concernées à l'exception des cas prévus par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

f) Tout produit informationnel issu de systèmes informatisés de Guide Succession et contenant de l'information confidentielle doit être conservé de façon sécuritaire et détruit ou mis au rebut selon les standards de sécurité, de confidentialité, et éventuellement d'archivage, lorsque sa détention ou son utilisation n'est plus nécessaire.

g) Lorsque le contrat avec un notaire prend fin, Guide Succession doit lui remettre (ou à son représentant autorisé), les actifs informationnels qui lui ont été confiés, sans en garder de copie.

Guide Succession doit détruire immédiatement sur ses équipements les données, sauf pour les copies de sauvegarde qui doivent être détruites après un cycle de sauvegarde ou un délai de 6 mois maximum, selon l'évènement qui se produit en premier.

h) Les médias, ou tout autre système ayant servi à offrir le service d'externalisation ou ayant contenu les données, qui ne servent plus à fournir le service d'externalisation, seront détruits de façon sécuritaire, par exemple, par la destruction physique du média ou par l'écriture multiple avec confirmation d'exécution. Guide Succession s'assure que les données qui y étaient contenues ne sont plus lisibles ni utilisables à d'autres fins.

3.3. Développement et maintenance des systèmes

3.3.1. Bon fonctionnement des applications

Des validations des paramètres d'entrée doivent être effectuées afin d'éviter l'injection de code (valeur hors limite, caractères spéciaux, requêtes SQL (« Structured Query Language »), chaîne de caractères volumineuse, etc.).

3.3.2. Mesures cryptographiques

a) À moins que d'autres mesures de sécurité comparables soient mises en place, les données sauvegardées chez Guide Succession doivent être chiffrées.
b) Les données doivent être chiffrées avant de quitter tout système informatique sous la responsabilité immédiate du notaire.
c) Un tunnel chiffré doit être utilisé entre les systèmes du notaire et ceux de Guide Succession pour sécuriser les données en transit.
d) L'algorithme de chiffrement utilisé doit être conforme aux meilleures pratiques sur le marché permettant d'assurer un bon niveau de protection. Toutefois, une méthode de recouvrement de la clé de chiffrement doit permettre de rendre les données accessible au notaire ou à la Chambre des Notaires ou à une personne autorisée en vertu de la loi, notamment un syndic de la Chambre des Notaires.

3.3.3. Sécurité des fichiers système

a) Tous les changements doivent être préalablement testés et approuvés avant d'être portés sur l'environnement de production.
b) Les serveurs et autres composantes critiques supportant le service d'externalisation doivent avoir fait l'objet d'un durcissement (« hardening ») de leur sécurité avant d'être mis en production.

3.3.4. Sécurité en matière de développement et d'assistance technique

L'information confidentielle ne doit pas être copiée dans les environnements de développement, de test et/ou de préproduction, à moins que ces environnements offrent des mesures de sécurité comparables à celles de l'environnement de production ou que les données aient été anonymisée.

3.3.5. Gestion des vulnérabilités techniques

Les systèmes et les applications doivent être configurés afin d'en assurer la sécurité. Uniquement les services ou les modules nécessaires doivent être actifs. Les correctif de sécurité, tant applicatifs que systèmes, doivent être testés et appliqués dans un délai raisonnable.

3.4. Droits de propriété intellectuelle

Les utilisateurs des actifs informationnels de Guide Succession doivent se conformer aux exigences légales sur l'utilisation de produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle. Plus spécifiquement :

a) Les reproductions de documents ne sont autorisées qu'à des fins de copies de sécurité ou selon la norme de la licence d'utilisation qui les régit;

b) Personne ne doit effectuer ou participer à la reproduction de documents sans le consentement du propriétaire du droit d'auteur;

3.5. Continuité des activités de l'organisation

3.5.1. Guide Succession doit disposer de mesures d'urgences en vue d'assurer la remise en opération des systèmes d'information, installations informatiques et de télécommunications institutionnelles.

3.5.2. Le fournisseur doit assurer la pérennité des données :

a) Mettre en place des alertes relatives aux formats d'encodage des données afin d'aviser la personne à l'origine du dépôt de l'obsolescence du format;
a) Assurer la disponibilité et l'accessibilité des données pour une période d'au moins 10 ans à partir de la date de sa création;
b) Assurer la pérennité des technologies supportant les données pour une période d'au moins 10 ans;

3.5.3. Aspect de la sécurité de l'information en matière de gestion de la continuité de l'activité

Le processus de gestion de la continuité des affaires est implanté afin de minimiser les impacts d'une non-disponibilité des données ou de service d'externalisation à un niveau acceptable par la Chambre des Notaires. Ces non-disponibilités pourraient être causées, par exemple, par un désastre naturel, un accident, un bris d'équipement ou du sabotage.

Le processus de continuité des affaires inclus les points suivants :

a) Identification des rôles et responsabilités;
b) Identification des procédures d'urgence;
c) Identification des procédures de recouvrement;
d) Identification des procédures de restauration;
e) Identification des procédures opérationnelle temporaire;
f) Identification des procédures de reprise des opérations normales;
g) Identification d'un niveau acceptable pour la perte d'information uo la non-disponibilité des services.
h) Documentation et mise en place des procédures de recouvrement et de restauration du service d'externalisation ou des données.
i) Inventaire des actifs informationnels (serveurs, logiciels, licences, etc.)
j) Test documenté des affaires et mise à jour du plan de continuité des affaires au moins une fois par année.

Une copie du plan de continuité de affaires est conservée au site de relève et une autre au site de production. Le niveau de sécurité concernant l'accès aux copies du plan de continuité doit être le même que celui pour l'accès au plan original. En tout temps, les copies doivent être conformes au plan original.

Le site de relève doit être situé à au moins 20 kilomètres du site de production.

3.6. Sensibilisation et formation

Tout partenaire d'affaires de Guide Succession doit être invité à prendre connaissance de la Politique de sécurité de l'information de Guide Succession. Cette politique devra être explicitement nommée dans les contrats et ententes faisant l'objet de documents officiels lorsque requis.

3.7. Droit de regard

Guide Succession a le droit de regard sur l'utilisation de ses actifs informationnels. Des vérifications doivent être effectuées périodiquement ou à la suite de demandes spécifiques. Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des utilisateurs et faire l'objet des règles suivantes :

a) Sauf en cas d'urgence manifeste, une vérification de l'utilisation des actifs informationnels et des équipements de télécommunications pour des raisons techniques, qui nécessiterait la lecture des informations personnelles et privées d'un usager, ne peut être effectuée que par des personnes autorisées, dans le cadre de leurs fonctions, après avoir prévenu la personne concernée et lui avoir donné l'opportunité de préserver ces informations;

b) Une vérification des informations personnelles d'un usager ou de l'utilisation des actifs par un usager ne peut pas être effectuée sans le consentement de ce dernier, sauf si Guide Succession a des raisons sérieuses et suffisantes de croire que l'usager utilise les actifs, systèmes ou réseaux en contravention aux lois.

3.8. Gestion des incidents liés à la sécurité de l'information

3.8.1. Signalement des évènements et des failles liés à la sécurité de l'information

Tout incident de sécurité relié à la sécurité de l'information pouvant avoir un impact sur la confidentialité, l'intégrité ou la disponibilité des données ou du service d'externalisation, sera rapporté à la Chambre des Notaires, plus spécifiquement au secrétaire de l'Ordre, notamment dans les cas suivants :

a) Une perte ou un vol d'informations en lien avec les clients, que cette menace se produise du côté du client ou de l'hébergeur
b) Une panne prolongée des systèmes servant à offrir le service d'hébergement de données
c) Une compromission (piratage) des systèmes de l'hébergeur.

3.9. Processus général de notification

Guide Succession s'engage à notifier aux utilisateurs et/ou aux personnes visées, par courriel ou tout autre moyen approprié selon la situation et ce, dans les meilleurs délais si un ou plusieurs des éléments suivants survenaient :

- Manquement à la politique;
- Panne ou mauvais fonctionnement de réseaux ou équipement;
- Mauvais fonctionnement des systèmes;
- Erreur humaine;
- Non-conformité avec une politique ou directive;

- Incident lié à la sécurité de l'information;

4. RÔLES ET RESPONSABILITÉS

4.1. Les administrateurs de Guide Succession

Le conseil d'administration de Guide Succession approuve la présente politique et s'assure de sa mise en œuvre. À cet égard, il autorise et approuve la Politique de sécurité de l'information et toutes les directives sous-jacentes. L'entreprise s'assure que les valeurs et les orientations en matière de sécurité de l'information soient partagées par tous les membres et partenaires d'affaires de Guide Succession. À cette fin, Guide Succession :

a) s'assure de l'application de la politique dans l'entreprise et par les fournisseurs de services;

b) Guide Succession est imputable du service d'externalisation, par conséquent, il est responsable de toutes les actions des tierces parties avec lesquelles il pourrait contracter;

c) apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique;

d) exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

4.2. La responsabilité des administrateurs et des tierces partie de Guide Succession

Chaque individu travaillant pour ou avec Guide Succession est responsable de respecter la présente politique ainsi que les directives et procédures en vigueur en matière de sécurité de l'information, et d'informer un membre du conseil d'administration de Guide Succession de toute violation des mesures de sécurité dont il pourrait être témoin ou de toutes anomalies décelées pouvant nuire à la protection des actifs informationnels. À cet effet, il :

a) Prend connaissance et adhère à la Politique de sécurité de l'information;

b) Utilise les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont autorisés;

c) Se conforme aux consignes et directives établies et dans le respect des dispositions de la présente politique.

5. DISPOSITIONS FINALES

5.1. Sanctions

Tout contrevenant à la présente politique et à la règlementation et directives internes qui en découlent s'expose, en plus des pénalités prévues aux Lois, aux sanctions suivantes en fonction de la nature, de la gravité et des conséquences de son geste :

a) annulation des droits d'accès aux équipements et services visés par la présente politique, sans avis ni délai, sous réserve des autres sanctions applicables;

b) remboursement à Guide Succession de toute somme que cette dernière serait dans l'obligation de défrayer suite à une utilisation non autorisée, frauduleuse ou illicite de ses services ou actifs informationnels;

c) mesure disciplinaire qui peut inclure une réprimande, une suspension, un congédiement ou toute autre sanction prévue ou imposée conformément aux conventions collectives de travail et aux protocoles en vigueur, selon les ententes contractuelles.

Le conseil d'administration est chargé de décider de l'opportunité d'appliquer l'une ou l'autre, ou plusieurs de ces sanctions. Elle peut également référer à toute autorité judiciaire les informations colligées sur tout utilisateur d'actif informationnel ayant contrevenu à cette politique et qui portent à croire qu'une infraction à l'une ou l'autre loi ou règlement en vigueur a été commise. Le contrevenant doit alors faire face à des mesures légales et s'expose à des poursuites judiciaires.

5.2. Modification / révision de la politique

Afin d'assurer son adéquation aux besoins de sécurité de Guide succession et s'ajuster aux nouvelles pratiques et technologies utilisées, la présente politique est révisée lors de tout changement important qui pourrait l'affecter.

Toute modification à la présente politique doit être sanctionnée par Guide Succession sur recommandation du conseil d'administration.

5.3. Mise en application et suivi de la politique

Conseil d'administration de Guide Succession est responsable de la mise en application et du suivi de la Politique de sécurité de l'information.

5.4. Date d'entrée en vigueur

La présente politique entre en vigueur à la date de son approbation par le conseil d'administration.

5.5. Durée

La présente politique prend effet pour l'utilisateur à sa date d'acceptation et demeurera en vigueur pour la période de l'abonnement au logiciel, à moins qu'elle ne soit annulée conformément aux lois ou résiliée conformément aux termes du contrat de licence de logiciel de Guide Succession.