

## ENTENTE DE FOURNITURE DE SERVICE D'EXTERNALISATION AUX NOTAIRES

ENTRE :

\*,\* société par actions régie par la \* *Loi sur les sociétés par actions*, constituée le \*, immatriculée au registraire des entreprises du Québec sous le numéro \*, ayant son siège au \*, province de Québec, \*, ci-après représentée par \* en sa qualité de \* dûment autorisé tel qu'il\* le déclare.

Ci-après nommée : le « **Fournisseur** ».

ET :

**CHAMBRE DES NOTAIRES DU QUÉBEC**, personne morale de droit public régie par le *Code des professions* et par la *Loi sur le notariat*, inscrite au fichier des autorités publiques sous le numéro 8814180590, ayant son siège au 2045, rue Stanley, suite 101, Montréal, province de Québec, H3A 2V4, représentée par M<sup>e</sup> **Stéphane Brunelle**, son **Directeur général**, aux termes d'une résolution du Comité exécutif adoptée à une séance du **18 novembre 2015**, laquelle est toujours en vigueur, n'ayant été ni modifiée, ni révoquée.

Ci-après nommée : la « **Chambre** ».

Le Fournisseur et la Chambre sont collectivement nommés : les « **Parties** ».

### LESQUELS DÉCLARENT CE QUI SUIT :

La Chambre a pour mission d'assurer la protection du public. Dans la poursuite de cette mission, elle peut imposer aux notaires des conditions, établir des normes de conservation, de gestion et de protection de leurs Documents technologiques et les imposer aux personnes qui entendent offrir un Service d'externalisation, telle que cette expression est définie à l'article 1.14 de la présente Entente.

## **EN CONSÉQUENCE, LES PARTIES CONVIENNENT DE CE QUI SUIT:**

### **1. DÉFINITIONS**

Les mots et expressions qui suivent ont, sauf si le contexte le requiert autrement, le sens qui leur est ci-après donné et ce, indépendamment du fait qu'ils débutent ou non par une lettre majuscule :

#### **1.1 « Annexe »**

désigne l'annexe au Contrat de service jointe aux présentes pour en faire partie intégrante.

#### **1.2 « Ayant droit »**

signifie toute personne ayant le pouvoir d'exercer un droit sur les Documents technologiques en vertu du Code des professions, de la Loi sur le notariat applicable et des règlements qui en découlent, notamment le syndic ou le secrétaire de la Chambre.

#### **1.3 « Contrat de service »**

signifie le contrat de fourniture de service d'externalisation aux notaires que le Fournisseur doit conclure avec le Notaire selon les modalités de la présente Entente, lequel prend la forme d'une licence d'utilisation contenant minimalement les dispositions de l'Annexe.

#### **1.4 « Directive de sécurité »**

signifie la « *Directive de sécurité - Fournisseurs de service d'externalisation aux notaires* » adoptée par la Chambre et en vigueur au moment de la signature de la présente Entente ainsi que chaque modification qui y sera apportée unilatéralement par la Chambre. Cette directive de sécurité régit le cadre de la sécurité des Documents technologiques et de leur accès, tant sur le plan administratif, technique que physique, sauf si le Fournisseur est certifié sous une Norme plus sévère ou contraignante ou se soumet volontairement au respect d'une telle Norme, auquel cas, cette dernière a préséance sur la Directive de sécurité. Une copie de la Directive est annexée à la présente Entente pour en faire partie intégrante.

#### **1.5 « Document technologique »**

signifie un document échangé, généré, produit, conservé ou transmis par un Notaire de quelque manière qu'il soit et dont le support fait appel aux technologies de l'information, au sens de la *Loi concernant le cadre juridique des technologies de l'information*, incluant toutes données, banques de données et métadonnées sous-jacentes qui en permettent la création. À titre d'exemple, il peut s'agir de Renseignements confidentiels, de renseignements personnels au sens des lois applicables en l'espèce, d'informations sur les clients, de courriels, de contrats ou d'ébauches d'avis juridique. Le Document technologique appartient au Notaire.

## **1.6 « Écrit »**

désigne tout écrit porté sur quelque support ou technologie que ce soit, le tout en conformité avec la liberté prévue à cet effet à l'article 2 de la *Loi concernant le cadre juridique des technologies de l'information*.

## **1.7 « Entente »**

signifie la présente entente, incluant le préambule, chaque document annexé à celle-ci et chaque modification ou ajout qui lui est apporté conformément à l'article 18. L'utilisation des termes « des présentes », « aux présentes », « par les présentes » dans l'entente, renvoie à cette dernière dans son ensemble.

## **1.8 « Force majeure »**

signifie l'intervention d'un événement extérieur, irrésistible et imprévisible, telle qu'une catastrophe naturelle, et qui empêche l'exécution d'une obligation.

## **1.9 « Norme »**

Signifie une norme plus sévère et plus contraignante que la Directive de sécurité, en matière de gouvernance et de sécurité des technologies de l'information, élaborée et mise à jour régulièrement par un organisme international compétent et reconnu par la Chambre, à laquelle le Fournisseur se soumet volontairement ou pour laquelle il détient une certification. \* Pour le Fournisseur, il s'agit de la norme \* en vertu de laquelle il est audité à tous les \* ans.\* [OU] Au moment de l'entrée en vigueur de l'Entente, le Fournisseur n'est pas certifié en vertu d'une Norme ni ne s'y soumet volontairement.

## **1.10 « Notaire »**

signifie la personne titulaire d'un permis d'exercice délivré par la Chambre, inscrite ou non au tableau de l'Ordre, qui utilise le Service d'externalisation et qui est partie à un Contrat de service, excluant la société au sein de laquelle un notaire exerce ses activités professionnelles.

## **1.11 « Nouveau service proposé »**

désigne toute nouvelle caractéristique ou fonctionnalité importante, tout logiciel, toute application ou tout service que le Fournisseur se propose d'incorporer au Service d'externalisation. Pour plus de précision, une simple amélioration des caractéristiques ou fonctionnalités du Service d'externalisation ne constitue pas un Nouveau service proposé aux fins des présentes.

### **1.12 « Partenaire »**

signifie indistinctement tout mandataire, sous-traitant, consultant, partenaire d'affaires, revendeur, prestataire de services ou entrepreneur du Fournisseur, ainsi que les partenaires de ces derniers.

### **1.13 « Renseignement confidentiel »**

signifie une information reçue par l'une des Parties, sous quelque forme et de quelque façon que ce soit, qui concerne l'une des Parties ou tout Notaire, ses employés, ses activités, ses produits ou ses procédés, sa clientèle ou ses fournisseurs et qui est désignée par l'une des Parties comme étant confidentielle ou qui doit être considérée comme étant confidentielle selon sa nature et les circonstances de la divulgation, incluant toute information sujette au secret professionnel.

### **1.14 « Service d'externalisation »**

signifie un service offert par un Fournisseur permettant à un Notaire de transférer ou de confier, peu importe le moyen, en tout ou en partie, ses Documents technologiques et ses ressources informatiques physiques ou logicielles. Ce service peut notamment être la sauvegarde des Documents technologiques à distance, l'hébergement d'équipements informatiques, l'exploitation d'un système d'information ou d'applications.

Dans le cas du Fournisseur, le « Service d'externalisation » consiste en un logiciel de \*, connu sous le nom de « \* ».

Toutefois, « Service d'externalisation » ne désigne pas \*.

« Service d'externalisation » signifie également tout Nouveau service proposé visé à l'article 8.5 et dont l'audit ne relève aucune non-conformité.

### **1.15 « Intervenante »**

désigne \*, personne morale constituée en vertu de \* en date du \*, ayant son siège au \*, agissant et représentée à la présente Entente par \*, président, et \*, vice-président et trésorier, dûment autorisés aux termes d'une résolution de leur conseil d'administration en date du \*, laquelle n'est pas modifiée ni révoquée. Une copie de cette résolution est annexée aux présentes, après avoir été reconnue véritable et signée pour identification par ces représentants en présence du notaire soussigné.

## **2. RÈGLES D'INTERPRÉTATION**

### **2.1 Lois applicables**

La présente Entente est régie et interprétée selon les lois en vigueur dans la province de Québec.

## **2.2 Titres**

Les titres utilisés dans la présente Entente ne le sont qu'à titre indicatif et ne peuvent servir à l'interprétation d'une disposition.

## **2.3 Genre et nombre**

Dans la présente Entente, un mot employé avec le genre masculin comprend le genre féminin et vice versa. À moins d'indication contraire, un mot employé au singulier comprend le pluriel et vice versa.

## **2.4 Devises canadiennes**

Une somme d'argent à laquelle il est fait référence dans la présente Entente est en devises canadiennes.

## **2.5 Divisibilité**

En cas de nullité de l'une des dispositions de la présente Entente, les autres dispositions conservent leur validité en y apportant les ajustements qui s'imposent.

## **2.6 Maintien des droits**

Le fait pour une partie de ne pas exercer un des droits prévus dans la présente Entente ne peut être interprété comme une renonciation à l'exercice d'un tel droit.

## **2.7 Préséance**

La présente Entente contient l'intégralité de l'Entente intervenue entre les Parties et exclut toute autre entente ou discussion antérieure à sa signature.

L'Entente a préséance sur toute disposition contraire ou incompatible contenue dans un autre document, sauf si cette dernière est plus sévère ou contraignante pour le Fournisseur.

L'Entente met fin à toute autre entente de fourniture de Service d'externalisation aux notaires intervenue entre les Parties.

## **2.8 Délais de rigueur**

Tous les délais prévus aux présentes sont de rigueur.

## **2.9 Absence de stipulation pour autrui**

La présente Entente ne doit en aucun cas être interprétée comme contenant une ou des stipulations pour autrui qui seraient faites en faveur de clients de Notaires.

### **3. OBJET DE L'ENTENTE**

La présente Entente autorise le Fournisseur à offrir le Service d'externalisation aux Notaires et en établit l'encadrement juridique.

### **4. OBLIGATIONS DU FOURNISSEUR**

- 4.1** Le Fournisseur doit être une personne morale régie en vertu d'une loi du Québec, du Canada ou d'une autre province ou territoire canadien. Son siège doit être situé au Canada. \* La personne morale doit en tout temps être contrôlée, directement ou indirectement, de quelque manière que ce soit, par des personnes physiques qui sont résidentes canadiennes aux fins fiscales ou de personnes morales constituées en vertu des lois ci-devant mentionnées et qui ont un siège au Canada.
- 4.2** Le Fournisseur doit maintenir son immatriculation en vertu de la *Loi sur la publicité légale des entreprises*, (RLRQ, c. P-44.1) et avoir une place d'affaires au Québec ou, à défaut, un fondé de pouvoir désigné qui y réside.
- 4.3** Le Fournisseur doit assurer la protection des Documents technologiques et celle du secret professionnel conformément aux dispositions de l'article 17.
- 4.4** Le Fournisseur doit :
- 4.4.1** Faire affaire avec des Partenaires qui respectent les mêmes standards de gouvernance et de sécurité des technologies de l'information que s'impose le Fournisseur, à savoir qu'ils soient certifiés en vertu de la Norme (ou d'une Norme équivalente) ou qu'ils s'y soumettent volontairement, le cas échéant et, subsidiairement, qu'ils respectent la Directive de sécurité;
- 4.4.2** Faire affaire avec un Partenaire possédant un site de production ou posséder un tel site, lequel doit être situé au Canada et s'assurer que les Documents technologiques soient conservés en territoire canadien;
- 4.4.3** Faire affaire avec un Partenaire possédant au moins un site de relève désigné pour le Service d'externalisation ou posséder au moins un tel site situé :
- i) à au moins vingt (20) kilomètres à vol d'oiseau du site de production; ou, alternativement;
  - ii) à un endroit préalablement autorisé par Écrit par la Chambre, dont la situation permet raisonnablement de croire qu'une même catastrophe (Force majeure ou non)

n'affecterait pas concurremment le site de production et le site de relève désigné pour le Service d'externalisation.

Il appartient au Fournisseur de faire la démonstration que sont réunies les conditions nécessaires à ii). La Chambre ne peut refuser son autorisation préalable que pour des motifs sérieux.

Tout site de relève désigné pour le Service d'externalisation doit être situé en territoire canadien.

- 4.4.4** Déclarer par Écrit à la Chambre tout changement dans les lieux dénoncés à l'article 5.2 au moins quatre-vingt-dix (90) jours avant sa survenance;
- 4.4.5** Assurer la disponibilité des Documents technologiques en moins de soixante-douze (72) heures en cas de Force majeure, ou dans les autres cas, selon le délai prévu à l'article 3 de l'Annexe;
- 4.4.6** Aviser préalablement le Notaire de la tenue de tout entretien planifié, de mise à niveau ou de toute autre opération du genre qui aura pour effet de rendre le Service d'externalisation indisponible.
- 4.5** Le Fournisseur déclare être certifié sous la norme \* depuis le \*, cette certification étant valide jusqu'au \*. À cet égard, le Fournisseur s'engage :
  - 4.5.1** \* À se conformer à toute modification subséquente à la Norme dans le délai déterminé conjointement par les Parties.  
\* [OU]  
\* À se conformer à toute modification à la Norme apportée à la suite de sa certification ou sa soumission volontaire, le cas échéant, dans le délai déterminé conjointement par les Parties.
  - 4.5.2** À aviser par Écrit la Chambre :
    - 4.5.2.1** \* Dans les cinq (5) jours, de son intention de se certifier ou de se soumettre volontairement à une Norme;
    - 4.5.2.2** \* Au moins quatre-vingt-dix (90) jours avant le moment où une certification en vertu de la Norme prendra fin, dans la mesure où il ne souhaite pas la renouveler ou, plus généralement, qu'il souhaite y mettre fin;

**4.5.2.2 \*** Dans les deux jours (2) suivant la prise de connaissance de l'intention de l'organisme certificateur de retirer, de révoquer ou, plus généralement, de mettre fin à une certification du Fournisseur.

**4.6** Le Fournisseur déclare avoir pris connaissance de la Directive de sécurité et s'engage à s'y conformer dans la mesure prévue aux présentes. Il s'engage également à se conformer à toute modification subséquente qui y serait faite par la Chambre.

Si des modifications à la Directive de sécurité impliquent des changements de quelque nature qu'ils soient de la part du Fournisseur, ce dernier s'engage à les effectuer dans un délai de trois (3) mois de la mise en vigueur des modifications ou, s'il est raisonnable de penser que l'importance des modifications requises requiert un délai plus important, par tout délai alors déterminé conjointement par les Parties.

**4.7** Transmettre à la Chambre, sans délai, sur le formulaire prescrit par cette dernière, un avis Écrit à l'effet qu'il a procédé aux changements nécessaires pour se conformer aux modifications à la Norme ou à la Directive de sécurité. Un tel formulaire complété constituera une déclaration du Fournisseur à l'effet que toutes les exigences sont respectées.

**4.8** Le Fournisseur doit conclure un Contrat de service avec le Notaire.

**4.9** Le Fournisseur s'engage à assurer le Service d'externalisation pendant toute la durée de l'Entente.

**4.10** Le Fournisseur doit individualiser, pour chaque Notaire, les Documents technologiques faisant l'objet du Service d'externalisation afin d'en protéger la confidentialité et le secret professionnel et d'en faciliter la gestion et l'accès.

**4.11** Le Fournisseur doit assurer la protection des Documents technologiques contre les accès non autorisés et ne pas les utiliser à d'autres fins que celles faisant l'objet du Contrat de service.

**4.12** Le Fournisseur doit conserver les Documents technologiques conformément à la Norme et la Directive de sécurité, le cas échéant, en plus d'en assurer le maintien, l'intégrité et l'accessibilité.

Cette obligation du Fournisseur ne doit toutefois pas être interprétée comme venant diminuer ou autrement alléger les obligations du Notaire aux termes de la loi, notamment, mais non limitativement, celles prévues au *Règlement sur la tenue des*



*dossiers et des études des notaires et au Règlement sur la comptabilité en fidéicommiss des notaires.*

**4.13** Le Fournisseur doit procéder, lorsque requis, à la remise des Documents technologiques conformément à l'article 11 de la présente Entente.

**4.14** Le Fournisseur s'engage à ne pas utiliser les logos de la Chambre.

Le Fournisseur s'engage également à ne pas alléguer, dans un message publicitaire, le fait d'être conforme aux exigences de la Chambre, d'être accrédité par la Chambre, d'être reconnu par la Chambre ou à alléguer toute autre affirmation semblable ou au même effet.

Nonobstant ce qui précède, le Fournisseur est autorisé à utiliser la formulation suivante : « Le Fournisseur est autorisé à offrir son service d'externalisation de documents technologiques aux notaires ».

Aux fins de ce qui précède, l'expression « message publicitaire » s'entend au sens de la *Loi sur la protection du consommateur*.

## **5. DÉCLARATIONS DU FOURNISSEUR**

### **5.1 Propriété intellectuelle**

Le Fournisseur déclare être propriétaire exclusif du Service d'externalisation et avoir obtenu toutes les autorisations ou licences requises de ses Partenaires pouvant avoir des droits ou des obligations dans le cadre de la prestation du Service d'externalisation.

Le Fournisseur déclare également que le Service d'externalisation est libre de droits moraux pouvant appartenir à des tiers.

Considérant ce qui précède, le Fournisseur reconnaît que la Chambre et les Notaires ne peuvent être tenus responsables des dommages ou pertes attribuables à des droits de propriété intellectuelle de Partenaires ou de tiers et dégage la Chambre et les Notaires de toute responsabilité à cet égard, directe ou indirecte.

Le Fournisseur doit défendre et indemniser la Chambre et le Notaire et les administrateurs, dirigeants et salariés de la Chambre et du Notaire et les dégager de toute responsabilité à l'égard de toute réclamation d'une tierce partie intentée contre la Chambre et/ou le Notaire, selon le cas, dans la mesure où cette réclamation : (i) concerne le Service d'externalisation; ou (ii) découle du travail effectué par le Fournisseur et/ou de ses Partenaires ou (iii) résulte de l'externalisation qui n'est pas conforme à l'Entente; ou (iv) découle de toute violation par le Fournisseur des termes et conditions des

présentes. Cet engagement du Fournisseur n'est valable qu'à condition que la Chambre et/ou le Notaire, selon le cas, informe le Fournisseur par Écrit de la réclamation en question, dans les quinze (15) jours ouvrables de sa connaissance, qu'elle laisse au Fournisseur la maîtrise exclusive de la défense dans le cadre de ladite réclamation et de toute négociation connexe visant la conclusion d'un règlement à l'amiable, qu'elle coopère avec le Fournisseur, et qu'elle aide ce dernier, à sa demande et à ses frais, à mener à bien cette défense.

Pour plus de précision, la connaissance d'une réclamation par le Notaire ne saurait signifier la connaissance de cette réclamation par la Chambre. Par ailleurs, le défaut du Notaire d'informer par Écrit la Chambre de l'existence d'une réclamation conformément au Contrat de service n'a pas pour effet de lui faire perdre ses droits aux termes de l'Entente.

Le Fournisseur pourra conclure un règlement à l'amiable à l'égard de toute réclamation qui est couverte par l'indemnité offerte aux termes de cet article sans l'approbation de la Chambre et/ou du Notaire, selon le cas, dans la mesure où ce règlement n'implique pas ou ne suggère pas une admission de responsabilité de la part de la Chambre et/ou du Notaire.

## 5.2 Équipements et infrastructures

Le Fournisseur déclare que son site de production est actuellement situé à l'endroit suivant : \* [Province], \* [Ville].

Le Fournisseur déclare de plus que son site de relève est actuellement situé à au moins vingt (20) kilomètres de son site de production, soit en \* [Province], \* [Ville].

\* Enfin, le Fournisseur déclare être le propriétaire exclusif des équipements et autres biens mobiliers corporels servant à l'exploitation du Service d'externalisation, à l'exception des sites de production et de relève qui appartiennent à son Partenaire \*. Le Fournisseur dispose des autorisations nécessaires pour utiliser et accéder aux sites de production et de relève.

\* [OU]

\* Enfin, le Fournisseur \* et l'Intervenante déclarent qu'ils sont les propriétaires exclusifs des équipements et autres biens mobiliers corporels servant à l'exploitation du Service d'externalisation (à l'exclusion des biens liés l'exploitation, effectuée chez un Partenaire du Fournisseur, de la solution de sauvegarde dont ce dernier est le seul propriétaire et qui est connue sous le nom de « \* »), dont la répartition de la propriété est établie entre eux, qu'ils sont les seuls à en avoir le contrôle et à pouvoir les sous-louer et conséquemment, qu'ils ont obtenu toutes les autorisations nécessaires afin de les utiliser et d'y accéder.

## **6. OBLIGATIONS DE LA CHAMBRE**

La Chambre s'engage à :

- 6.1** Publier sur son site Internet, sur l'Espace notaire ou tout autre outil de communication semblable, l'existence de la présente Entente, un modèle d'Entente et la Directive de sécurité, de même que toutes modifications au modèle et à la Directive, le cas échéant, dans les trente (30) jours de leur entrée en vigueur; et
- 6.2** Faire preuve d'impartialité dans le traitement des différents fournisseurs d'un Service d'externalisation, dans l'interprétation et l'application du texte de l'Entente et de la Directive de sécurité. Pour plus de précision, le fait de ne pas conclure les ententes simultanément avec tous les fournisseurs ne constitue pas une source de partialité.

## **7. CONTRAT DE SERVICE AVEC LE NOTAIRE**

- 7.1** En plus de tout autre contrat en vigueur entre le Fournisseur et le Notaire (et/ou avec la société par l'entremise de laquelle le Notaire exerce sa profession), le Fournisseur doit conclure un Contrat de service distinct avec chaque Notaire à qui le Service d'externalisation est rendu.
- 7.2** Le Fournisseur s'engage à modifier tous les Contrats de service et à y faire adhérer les Notaires dans les quatre-vingt-dix (90) jours de la signature de la présente Entente ou d'une nouvelle Entente avec la Chambre si de telles modifications sont requises pour donner plein effet aux présentes.

Toute contravention aux dispositions de l'article 7 obligera le Fournisseur à payer à la Chambre une somme de cinq cents dollars (500 \$) par Contrat de service non conforme à titre de dommages et intérêts liquidés, le tout, sans préjudice à tous autres recours qui pourraient être exercés simultanément ou séparément par la Chambre.

## **8. AUDITS ET DÉCLARATIONS ANNUELLES**

Le Fournisseur et la Chambre conviennent que tout audit effectué en application du présent article vise à vérifier que le Fournisseur satisfait aux exigences de l'Entente, d'une Norme et de la Directive de sécurité, dans la mesure où cette dernière est applicable.

## 8.1 Audit préalable

Le Fournisseur et la Chambre déclarent qu'un audit de sécurité simplifié a été effectué préalablement à la signature des présentes soit au cours \* de/\* du \* l'\* été/l'automne/l'hiver/printemps aux frais du Fournisseur. Un rapport de l'audit daté du \* a été transmis à la Chambre qui reconnaît l'avoir reçu.

\* Ce rapport recommandait l'autorisation du Service d'externalisation par le Fournisseur.

\* [OU]

\* Ce rapport recommandait l'autorisation du Service d'externalisation par le Fournisseur, sous réserve de conditions spécifiques que ce dernier s'est engagé à réaliser en vertu de l'article 4 des présentes.

## 8.2 Audit en vertu d'une Norme

Dans l'éventualité où, à tout moment pendant la durée de l'Entente, le Fournisseur serait certifié en vertu d'une Norme ou se soumettrait volontairement, à ses frais, à un processus d'audit de ses contrôles et mesures de sécurité de l'information en vertu d'une Norme, le Fournisseur fournira sans frais à la Chambre un exemplaire lui étant adressé de tout rapport d'audit en résultant.

Sur réception d'un tel rapport d'audit, la Chambre pourra, aux frais du Fournisseur, mandater un auditeur de son choix afin de :

- i) poser des questions en regard du contenu du rapport d'audit et du plan de correction des non-conformités, le cas échéant, auxquelles le Fournisseur devra fournir les informations additionnelles;
- ii) valider la conformité des exigences de l'Entente et de la Directive de sécurité qui ne seraient pas couvertes par la Norme.

L'audit devra être réalisé à une fréquence équivalente à celle prévue par la Norme. Le Fournisseur non certifié en vertu de la Norme qu'il souhaite respecter doit minimalement être audité tous les trois (3) ans, tel que prévu à l'article 8.4. L'audit doit être réalisé par une firme renommée, indépendante et acceptable pour la Chambre.

## 8.3 Changement d'auditeur ou fin de l'audit en vertu d'une Norme

Le Fournisseur doit aviser par Écrit la Chambre de son intention de changer d'auditeur ou d'abandonner l'audit en vertu d'une Norme dont il est question à l'article 8.2 au moins quatre-vingt-dix (90) jours avant le moment où le prochain audit se déroulera ou, selon le cas, se serait

déroulé si le Fournisseur avait eu l'intention de poursuivre les audits en vertu d'une Norme.

Le préavis Écrit indiquera les motifs à la base de ce changement ou abandon, selon le cas.

#### **8.4 Processus d'audit en vertu de la Directive de sécurité**

Dans la mesure où à tout moment pendant la durée de la présente Entente, le Fournisseur abandonne l'audit en vertu d'une Norme prévu à l'article 8.2, le Fournisseur consent à ce qu'un audit soit réalisé à ses frais, à la demande de la Chambre, au plus tard à la date d'anniversaire du dernier audit en vertu d'une Norme et par la suite, une (1) fois à chaque période de trois (3) ans.

Un auditeur mandaté par la Chambre sera chargé à cet effet de valider que le Fournisseur satisfait aux exigences de la présente Entente et de la Directive de sécurité dans un « Rapport d'assurance raisonnable concernant la déclaration sur la conformité » en vertu de la norme NCMC 3530 qui lui sera adressé.

L'auditeur pourrait également être choisi par le Fournisseur et agréé par la Chambre, qui exigera alors des garanties quant à sa renommée et son indépendance.

Tout audit en vertu du présent article doit être précédé d'un avis d'au moins vingt (20) jours ouvrables.

Dans tous les cas, l'audit pourra, à la discrétion de la Chambre, être effectué aux places d'affaires du Fournisseur pendant ses heures d'affaires.

Ce processus d'audit obligatoire aura cours tant que le Fournisseur ne reprendra pas le processus d'audit en vertu d'une Norme de l'article 8.2.

#### **8.5 Audit d'un Nouveau service proposé**

Tout Nouveau service proposé devra faire l'objet d'une déclaration écrite du Fournisseur à la Chambre sur le formulaire prescrit à cet effet et ce, avant qu'il ne soit offert aux Notaires et incorporé au Service d'externalisation.

Sur la base de l'information reçue, la Chambre pourra, à son entière discrétion, exiger qu'un audit soit réalisé aux frais du Fournisseur. Cet audit aura pour objet de confirmer la conformité du Nouveau service proposé avec l'Entente, la Norme et la Directive de sécurité, et ne devra relever aucune non-conformité.

Si aucun audit n'est requis, la mention « et dont l'audit ne relève aucune non-conformité » contenue à l'article 1.14 sera réputée non écrite.

### **8.6 Audits ponctuels**

Malgré les dispositions précédentes, un audit ponctuel peut être effectué aux frais de la Chambre, à la suite d'un incident lié à la sécurité, tel que prévu à l'article 9 ou pour tout autre motif raisonnable.

### **8.7 Confidentialité et respect du secret professionnel**

La Chambre peut, dans le cadre de tout audit, effectuer toute vérification relative à la confidentialité et au secret professionnel et par voie de conséquence, au respect des conditions mentionnées à l'article 17 des présentes. La Chambre peut aussi effectuer un audit uniquement pour ces fins.

### **8.8 Non-conformités**

Une vérification des non-conformités relevées lors d'un audit ou d'un incident lié à la sécurité pourra être faite par la Chambre aux frais du Fournisseur afin de s'assurer qu'elles sont corrigées ou qu'elles le seront dans un délai raisonnable convenu entre les Parties.

Toutefois, la Chambre ne peut exiger du Fournisseur de corriger une non-conformité soulevée à la suite d'un incident de sécurité, d'un audit ou dans une déclaration annuelle prévue à l'article 8.9 que dans les douze (12) mois de l'avis d'incident ou de la réception du rapport d'audit ou de la déclaration annuelle par la Chambre.

À défaut par la Chambre d'exiger la correction d'une non-conformité dans le délai précité, le Fournisseur pourra néanmoins volontairement accepter d'effectuer cette correction.

### **8.9 Déclaration annuelle**

Le Fournisseur s'engage à ses frais à retourner à la Chambre, annuellement, à la date d'anniversaire de la présente Entente ou à tout autre moment mutuellement convenu entre les Parties, une déclaration Écrite de la direction portant sur le respect de de l'Entente, de la Norme et de la Directive de sécurité, la version du Service d'externalisation et les changements d'importance de la dernière année, ainsi que les changements dans ses Partenaires, lieux d'hébergement, de sauvegarde et de relève des Documents technologiques.

Cette déclaration peut être incluse dans le rapport d'audit effectué en vertu du présent article.

### **8.10 Audit d'un Partenaire**

Pendant la durée de l'Entente, le Fournisseur devra fournir sans frais à la Chambre, une fois par année, les extraits rendus disponibles des rapports d'audit des contrôles internes et des mesures de sécurité de tout Partenaire hébergeant, traitant ou ayant quelque autre accès aux Documents technologiques.

Un audit ponctuel d'un Partenaire du Fournisseur hébergeant, traitant ou ayant quelque autre accès aux Documents technologiques peut être effectué aux frais de la Chambre, à la suite d'un incident lié à la sécurité, tel que prévu à l'article 9 ou pour tout autre motif raisonnable se rapportant au Service d'externalisation. Le Fournisseur promet que son Partenaire consentira à un tel audit, la présente constituant une promesse du fait d'autrui au sens du *Code civil du Québec*. Le Fournisseur s'engage à insérer, dans tout contrat conclu avec un Partenaire après la date des présentes, une stipulation en faveur de la Chambre à cet effet.

Une vérification des non-conformités relevées lors d'un audit ou d'un incident lié à la sécurité pourra être faite afin de s'assurer qu'elles sont corrigées ou qu'elles le seront dans un délai raisonnable convenu entre les Parties et le Partenaire.

### **8.11 Tests applicatifs**

Le Fournisseur devra fournir sans frais à la Chambre les résultats de tous tests de vulnérabilité et de pénétration applicatifs réalisés de temps à autre pendant la durée de l'Entente. La déclaration annuelle prévue à l'article 8.9 fera état de l'existence ou de l'inexistence de tels tests.

### **8.12 Maintien de la responsabilité**

Tout contrôle effectué en vertu de la présente Entente ne dégage pas pour autant le Fournisseur de ses responsabilités à l'égard de son exécution et de la prestation du Service d'externalisation.

## **9. GESTION DES CHANGEMENTS ET DES INCIDENTS LIES A LA SECURITÉ**

En cas de changement ou d'incident lié à la sécurité, tel que défini à la Directive de sécurité, le Fournisseur doit aviser la Chambre selon la procédure suivante :

- 9.1** Un changement qui peut avoir un impact sur le respect de la Norme et de la Directive de sécurité, de quelque nature qu'il soit, doit être signalé à la Chambre au moins trente (30) jours avant l'entrée en vigueur du changement afin qu'elle puisse en analyser, à l'intérieur de ce délai, les risques ou les impacts et ainsi déterminer si la

demande de changement est conforme à la Norme et à la Directive de sécurité.

À défaut pour la Chambre d'agir à l'intérieur du délai de trente (30) jours précité, elle sera réputée avoir accepté le changement.

- 9.2** Le Fournisseur doit, conformément aux modalités prévues à la Directive de sécurité, aviser la Chambre d'un incident lié à la sécurité qui peut avoir un impact sur l'intégrité, la confidentialité, le secret professionnel ou la disponibilité des Documents technologiques. Cet avis doit être transmis dans les quarante-huit (48) heures qui suivent sa détection.

## **10. ACCESSIBILITE**

Le Fournisseur doit, en tout temps, sous réserve des dispositions de l'article 4.4.5, rendre les Documents technologiques accessibles au Notaire ou à la Chambre conformément à la loi ou à une personne autorisée en vertu de la loi, notamment un syndic de la Chambre.

La Chambre n'a pas à justifier son droit d'accès. Le Fournisseur doit obtempérer sur demande.

L'accessibilité par la Chambre ou par la personne autorisée s'effectue à partir d'une connexion internet via l'application \* , en mode lecture exclusivement. Les Documents technologiques auxquels un syndic de la Chambre a accès peuvent être téléchargés par lui.

## **11. REMISE DES DOCUMENTS TECHNOLOGIQUES PAR LE FOURNISSEUR**

**11.1** Le Fournisseur doit rendre disponible les Documents technologiques à l'une ou l'autre des personnes suivantes, selon les circonstances ci-après décrites :

- a) au Notaire ou aux Ayants droit, selon le cas, lors de la résiliation du Contrat de service, sur simple demande;
- b) à un nouveau Fournisseur désigné par le Notaire ou par les Ayants droit lors de la résiliation du Contrat de service, sur simple demande et, dans le cas des Ayants droit, sur justification de leur titre;
- c) si le Fournisseur cesse d'offrir le Service d'externalisation pour quelque raison que ce soit sans qu'un autre fournisseur ne poursuive son exploitation \* ou ne soit désigné par l'Intervenante conformément à l'article 15 immédiatement après cette cessation conformément aux dispositions des présentes, au fournisseur désigné par la Chambre sur demande de son secrétaire;



- d) à toute personne autorisée par la loi ou par la Chambre, notamment au syndic de la Chambre, à recevoir ces Documents technologiques en vertu de la loi et des règlements qui régissent la profession notariale, sur simple demande.

Pour plus de précision, une telle demande peut être effectuée après la résiliation de l'Entente, sujet toutefois à la destruction des Documents technologiques prévue à l'article 12.

**11.2** L'intégralité des Documents technologiques en possession d'un Fournisseur doit dans tous les cas être disponible de façon sécuritaire et au plus tard dans un délai de quinze (15) jours de la demande. Le Fournisseur qui souhaite facturer quelques frais ou honoraires que ce soit au Notaire relativement à la remise des Documents technologiques de ce dernier ne peut en exiger le paiement tant que cette remise n'est pas entièrement complétée.

**11.3** Si le Fournisseur décide de cesser d'offrir le Service d'externalisation aux Notaires, il doit en aviser la Chambre au plus tard quatre-vingt-dix (90) jours avant la date prévue de la cessation du Service d'externalisation. Telle cessation entraînera la résiliation de la présente Entente. Le Fournisseur doit alors remettre tous les Documents technologiques faisant l'objet du Service d'externalisation conformément à ce qui précède.

## **12. DESTRUCTION DES DOCUMENTS TECHNOLOGIQUES PAR LE FOURNISSEUR**

**12.1** Le Fournisseur doit détruire tous les exemplaires de Documents technologiques (en production, redondance et sauvegarde) de façon sécuritaire, de la manière prévue à la Directive de sécurité, peu importe le support sur lequel ils se trouvent, en fonction de ce qui est prévu au présent article.

**12.2** Le Fournisseur ne peut détruire les Documents technologiques avant d'avoir transmis au Notaire un préavis Écrit de 60 jours lui précisant la marche à suivre afin de les récupérer.

**12.3** Le Fournisseur doit détruire tous les Documents technologiques d'un Notaire au plus tard 120 jours après la réception par le Notaire du préavis Écrit de l'article 12.2.

**12.4** Une fois la présente Entente terminée, le Fournisseur s'engage à produire à la Chambre un avis Écrit confirmant :

**12.4.1** Qu'il a remis ou déployé des efforts raisonnables afin de remettre les Documents technologiques aux personnes y ayant droit;

**12.4.2** Qu'il a effectué la destruction totale et irréversible de tous les exemplaires des Documents technologiques (en production, redondance et sauvegarde) conformément à l'article 12.1. Les

droits d'audits de la Chambre, dans ce contexte de fin d'Entente, comprendront celui d'effectuer toute vérification à cet effet.

### **13. ASSURANCES**

Le Fournisseur doit souscrire et maintenir en vigueur pendant la durée de l'Entente, à ses frais et auprès de compagnies d'assurance reconnues, des polices d'assurance des types et pour les montants de couverture ci-après mentionnés comportant des franchises d'un montant maximum de DIX MILLE DOLLARS (10 000 \$) :

**13.1** Assurance générale d'entreprise sur les biens couvrant le contenu et les biens matériels qui sont affectés à la prestation du Service d'externalisation pour garantir les pertes et les dommages causés par le feu, l'eau, le vol et le vandalisme pour le plein montant de la valeur de remplacement des biens.

**13.2** Assurance responsabilité civile qui doit avoir une limite minimale de deux millions de dollars (2 000 000 \$) par sinistre.

**13.3** Assurance offrant une couverture cyber-risques couvrant minimalement :

- La responsabilité pour des atteintes à la sécurité des réseaux informatiques, de l'information et de la confidentialité des renseignements personnels;
- La protection des actifs informationnels ou produits technologiques;
- Le remboursement des frais liés à la gestion des incidents affectant la sécurité des réseaux informatiques, l'information et la confidentialité des renseignements personnels, incluant les services professionnels et technologiques des tiers;
- Les frais de défense, les frais d'enquête et une garantie à l'encontre des pénalités administratives;
- La cyber-extorsion.

Chacune des garanties mentionnées à l'article 13.3 devant faire état d'une limite de deux millions de dollars (2 000 000 \$) par sinistre et de cinq millions de dollars (5 000 000 \$) par période annuelle.

### **14. CESSION**

**14.1** Le Fournisseur ne peut céder, en tout ou en partie, de façon directe ou indirecte, aucun des droits ou obligations prévus aux présentes ou dans tout Contrat de service sans au préalable avoir obtenu l'autorisation de la Chambre, laquelle ne peut refuser que pour des motifs sérieux. Constitue, notamment, mais non limitativement, un

motif sérieux de refus, le fait que l'acquéreur ne s'engage pas à l'égard de la Chambre à respecter toutes les obligations, les conditions et les modalités de l'Entente.

Nonobstant ce qui précède, le Fournisseur peut céder en totalité les droits et obligations prévus aux présentes et dans tout Contrat de service sans au préalable avoir obtenu l'autorisation de la Chambre à la condition expresse que cette cession soit faite en faveur d'une personne, fiduciaire ou société de personnes ayant, au moment de la cession et en tout temps par la suite, un lien de dépendance avec le Fournisseur au sens de l'article 251 de la *Loi de l'impôt sur le revenu*, mais en ne tenant pas compte, c'est-à-dire comme si elles n'existaient pas, des présomptions prévues au paragraphe 5 de cet article. Dans un tel cas toutefois, le Fournisseur devra se porter caution solidaire des obligations du cessionnaire aux termes de l'Entente suivant les modalités usuelles en pareille matière.

Aux fins de ce qui précède mais sous réserve de ce qui suit, une acquisition de contrôle du Fournisseur sera réputée constituer une cession de ses droits dans la présente Entente.

Toutefois, une acquisition de contrôle du Fournisseur par une personne, fiduciaire ou société de personnes ayant, au moment de l'acquisition et en tout temps par la suite, un lien de dépendance avec le Fournisseur au sens de l'article 251 de la *Loi de l'impôt sur le revenu*, mais en ne tenant pas compte, c'est-à-dire comme si elles n'existaient pas, des présomptions prévues au paragraphe 5 de cet article, ne sera pas réputée constituer une cession de ses droits dans la présente Entente.

**14.2** Le Fournisseur doit aviser la Chambre de son intention au moins quatre-vingt-dix (90) jours avant la date prévue de la cession.

**14.3** La Chambre doit y répondre dans les quarante-cinq (45) jours suivant la réception de l'avis. Dans le cas d'un refus, la Chambre doit faire part de ses motifs par Écrit. À défaut pour la Chambre de répondre à l'intérieur du délai de quarante-cinq (45) jours, la Chambre sera réputée avoir consenti à la cession.

## **15. PARTICULARITÉS PROPRES À LA RELATION INTERVENANTE-FOURNISSEUR**

En raison des particularités de la relation contractuelle entre l'Intervenante et le Fournisseur, les Parties et l'Intervenante conviennent de ce qui suit, nonobstant toute autre disposition des présentes, les dispositions du présent article 15 ayant par ailleurs préséance sur toute autre disposition incompatible des présentes.

- 15.1** Le droit de cession du Fournisseur visé à l'article 14.1 et se rapportant au logiciel connu sous le nom de « \* » est dans tous les cas, conditionnel à l'approbation écrite préalable de l'Intervenante. À défaut, elle ne peut avoir lieu. L'Intervenante s'engage, dans les meilleurs délais, à communiquer à la Chambre une copie de toute approbation donnée, le cas échéant.
- 15.2** Les Parties reconnaissent que, sujet aux modalités contenues aux contrats intervenus entre le Fournisseur et l'Intervenante, cette dernière peut confier la licence du logiciel connu sous le nom de « \* » à un autre fournisseur. Dans un tel cas, le Fournisseur reconnaît que les dispositions prévues à l'article 11, relative à la remise des Documents technologiques, s'appliqueront alors avec les adaptations nécessaires en faveur du nouveau fournisseur désigné par l'Intervenante. Toutefois, une telle remise ne pourra pas être effectuée et sera suspendue tant et aussi longtemps que le nouveau Fournisseur désigné par l'Intervenante n'aura pas adhéré à la présente Entente (ou à toute autre version alors en vigueur).
- 15.3** Dès que l'adhésion du nouveau fournisseur à la présente Entente et la remise des Documents technologiques en sa faveur seront complétés, l'Entente sera résiliée à l'égard du Fournisseur comparissant aux présentes en ce qui concerne le logiciel connu sous le nom de « \* ». Le Fournisseur devra alors procéder à la destruction des Documents technologiques à l'expiration du sixième (6<sup>e</sup>) mois suivant leur remise. L'Entente demeurera toutefois pleinement en vigueur et exécutoire en ce qui concerne la solution connue sous le nom de « \* » et devra dès lors se lire avec les adaptations nécessaires.
- 15.4** Une copie de tout avis de résiliation prévu à l'article 20 devra être envoyée à l'Intervenante selon les mêmes délais prévus à cet article.
- 15.5** Les droits et obligations du Fournisseur prévus à l'article 17 et à l'article 22 sont également souscrits personnellement par l'Intervenante en y faisant les adaptations nécessaires, notamment, mais non limitativement, d'inclure l'Intervenante comme « partie » au sens de la définition de « Renseignement confidentiel ».

## **16. INSAISSABILITE**

Outre les exemptions prévues au *Code de procédure civile* du Québec, le Fournisseur reconnaît l'insaisissabilité du greffe du Notaire, ses classeurs, ses dossiers, ses livres de droit et autres documents d'ordre professionnel, ainsi que ses registres et ses pièces de comptabilité, de même que les

Documents technologiques qui y sont reliés et les supports faisant appel aux technologies de l'information qui sont reliés à l'exercice de la profession notariale.

## **17. CONFIDENTIALITÉ**

### **17.1 Renseignement confidentiel**

Un Renseignement confidentiel demeure la propriété de la Partie qui le divulgue.

Les Parties s'engagent à ne pas utiliser, ni divulguer un Renseignement confidentiel sauf aux personnes pouvant y avoir droit et aux seules fins de l'exécution de la présente Entente.

Chaque Partie s'engage à ce que ni elle, ni aucun des membres de son personnel, ses agents, Partenaires, représentants ou dirigeants divulguent ou utilisent, sans y être dûment autorisée par l'autre Partie, les renseignements, les Documents technologiques, les analyses ou les résultats inclus dans les rapports réalisés en application de la présente Entente ou, généralement, quoi que ce soit dont elle aurait eu connaissance dans l'exécution de la présente Entente.

Pour plus de précision, la Chambre pourra utiliser à ses propres fins tout ou partie des Renseignements confidentiels qui lui sont communiqués par le Fournisseur, en application de la présente Entente.

Chaque Partie s'engage à prendre les mesures nécessaires pour que chaque personne visée par l'exécution de la présente Entente ne divulgue ou ne porte à la connaissance de qui que ce soit et qu'elle n'utilisera pas un Renseignement confidentiel à son avantage personnel ou pour le bénéfice d'une autre personne.

Chaque Partie est responsable de tout dommage pouvant découler du non-respect du caractère confidentiel d'un renseignement en sa possession. À ce titre, chaque Partie se porte garante de tous ses employés, agents, Partenaires, représentants ou dirigeants.

### **17.2 Secret professionnel**

Le Fournisseur reconnaît expressément que de nombreux Documents technologiques qui lui sont transmis dans le cadre du Service d'externalisation, sont protégés par le secret professionnel du Notaire.

Le Fournisseur reconnaît que ce secret professionnel est un principe fondamental dans notre droit et tire sa source de divers lois et règlements, notamment, mais non limitativement, les suivants :

- *Charte des droits et libertés de la personne*, RLRQ, c. C-12, art. 9;

- *Loi sur le notariat*, RLRQ, c. N-3, art. 14.1;
- *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 3 et 33;
- *Code de déontologie des notaires*, RLRQ, c. N-3, r. 2.

Par conséquent, aux fins de parfaire l'engagement du Fournisseur aux termes de l'article 4.3 de l'Entente, le Fournisseur s'engage à :

- Se comporter de façon à protéger le secret professionnel des Documents technologiques qui lui sont transmis par le Notaire;
- Limiter l'accès aux Documents technologiques protégés par le secret professionnel aux personnes qui doivent absolument y avoir accès, les informer du fait que les Documents technologiques sont ainsi protégés par le secret professionnel et leur faire souscrire un engagement Écrit à se comporter de façon à protéger le secret professionnel de ces Documents technologiques;
- Aviser sans délai le Notaire de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité (incluant les dispositions de l'article 17.1) et relatives à la protection du secret professionnel et ce, tant à l'égard de violations contractuelles que de celles qui pourraient découler de l'application d'une loi, notamment, mais non limitativement, de toutes lois fiscales. Cette disposition à préséance sur le l'article 9.2.

Le présent article ne doit en aucun temps être interprété comme limitant ou restreignant la portée générale des autres dispositions de l'Entente, notamment, des dispositions de l'article 17.1.

### **16.3 Respect du secret d'enquête**

Le Fournisseur s'engage à ne pas divulguer au Notaire avec qui il contracte la prestation du Service ni à qui que ce soit d'autre, l'existence d'une enquête de la part de la Chambre ou d'une demande de la part d'un représentant de la Chambre, notamment le syndic, ni les Documents technologiques qui ont été remis à ce dernier.

Le Fournisseur s'engage à faire en sorte que ses employés, agents, Partenaires, représentants ou dirigeants respectent cette obligation.

## **18. MODIFICATION DE L'ENTENTE**

La présente Entente peut être modifiée en tout temps d'un commun accord entre les Parties. Toute modification doit toutefois être consignée par Écrit et signée par chacune des Parties. Elle est présumée prendre effet le jour où elle est consignée dans un Écrit, sauf stipulation contraire des Parties.

## **19. DURÉE ET ENTRÉE EN VIGUEUR**

La présente Entente est à durée indéterminée et entre en vigueur le \*\*, malgré sa date de signature par les Parties.

## **20. RÉSILIATION DE L'ENTENTE**

- 20.1** Outre les motifs prévus aux autres dispositions des présentes, la présente Entente peut être résiliée par l'une ou l'autre des Parties sans motif en donnant un avis à l'autre Partie d'au moins quatre-vingt-dix (90) jours de la date de résiliation.
- 20.2** Si le Fournisseur est en défaut de conclure des Contrats de service contenant toutes les dispositions contenues à l'Annexe ou si les modifications prévues à l'article 7.2 n'ont pas été complétées dans les délais prévus, la Chambre peut, sans préjudice à ses autres recours, résilier l'Entente au moyen d'un préavis au Fournisseur. La présente Entente sera alors résiliée automatiquement à la dixième (10<sup>e</sup>) journée suivant l'envoi du préavis.
- 20.3** Si le Fournisseur ne respecte pas une obligation de l'Entente et qu'il n'y remédie pas dans les délais requis aux termes d'un avis de la Chambre à cet effet, la Chambre peut, sous réserve de ses autres recours, résilier l'Entente au moyen d'un préavis au Fournisseur. La présente Entente sera alors résiliée automatiquement à la quarante-cinquième (45<sup>e</sup>) journée suivant l'envoi de l'avis.
- 20.4** Si le Fournisseur devient failli ou insolvable, la Chambre peut, sous réserve de ses autres recours, résilier l'Entente au moyen d'un préavis au Fournisseur. La présente Entente sera alors résiliée automatiquement à la septième (7<sup>e</sup>) journée suivant l'envoi de l'avis.
- 20.5** Si le Fournisseur contrevient à toute directive de Solutions Notarius Inc. et/ou Notarius - technologies et systèmes d'information notariale Inc. relative à l'utilisation de la signature numérique, la Chambre peut, sans préjudice à ses autres recours, résilier l'Entente au moyen d'un préavis au Fournisseur dénonçant la contravention alléguée. La présente Entente sera alors résiliée automatiquement à la dixième (10<sup>e</sup>) journée suivant l'envoi du préavis sauf si la contravention alléguée est remédiée dans ce délai.
- 20.6** La fin de la présente Entente met un terme à tout Contrat de service, le tout, sans possibilité pour le Fournisseur et/ou le Notaire d'exiger de dommages-intérêts de la Chambre ou quelque autre compensation que ce soit de sa part.

## 21. SURVIE DES DROITS ET DES OBLIGATIONS

Les droits et obligations des Parties prévus aux articles suivants survivent à la fin de la présente Entente pour la durée indiquée :

- 21.1 Sécurité, protection, destruction des Documents technologiques (articles 4.3, 4.10, 4.11, 12 et 17) : les droits et obligations des Parties s'éteindront par la production par le Fournisseur à la Chambre de l'avis Écrit de l'article 12.4 confirmant la destruction totale et irréversible des Documents technologiques conformément à l'article 12.1 des présentes.
- 21.2 Confidentialité, secret professionnel, secret d'enquête (articles 4.3, 4.10, 4.11 et 17) : les droits et obligations des Parties survivent perpétuellement.
- 21.3 Défense et indemnisation (article 5.1) : les droits et obligations des Parties s'éteindront à l'expiration d'un délai de trois (3) ans suivant la date de fin de la présente Entente.
- 21.4 Audits et déclarations annuelles (article 8) : les dispositions de l'article 8 s'appliqueront *mutatis mutandis* pour la période s'échelonnant entre la date du dernier audit effectué et la date de fin de l'Entente. Pour plus de précision, en cas d'application de l'article 8.2, cela ne signifie pas que le Fournisseur doit accélérer la réalisation de l'audit prévu par ses accréditations ou certifications, mais plutôt qu'il devra fournir à la Chambre, malgré la fin de l'Entente, le rapport d'audit des contrôles et mesures de sécurité de l'information couvrant la période s'échelonnant entre la date du dernier audit effectué et la date de fin de l'Entente.
- 21.5 Avis relatif à un Incident de sécurité (article 9.2) : les droits et obligations ne s'éteindront que par la production par le Fournisseur à la Chambre de l'avis Écrit de l'article 12.4 confirmant la destruction totale et irréversible des Documents technologiques conformément à l'article 12.1 des présentes.
- 21.6 Remise des Documents technologiques (article 11) : les droits et obligations ne s'éteindront que par la production par le Fournisseur à la Chambre de l'avis Écrit de l'article 12.4 confirmant la remise ou le déploiement d'efforts raisonnables de remise des Documents technologiques aux personnes y ayant droit.
- 21.7 Assurances (article 13) : les droits et obligations des Parties s'éteindront à l'expiration d'un délai de trois (3) ans suivant la date de fin de la présente Entente.



**21.8** Clause compromissoire (article 22) : les droits et obligations des Parties survivent perpétuellement.

**21.9** Avis (article 23) : les droits et obligations des Parties survivent perpétuellement.

## **22. CLAUSE COMPROMISSOIRE**

Les Parties incluant aux fins du présent article, l'Intervenante conviennent que toute réclamation issue de la présente Entente faisant l'objet d'une contestation, tout différend concernant l'exécution ou l'inexécution de celle-ci, y compris son annulation, sa résiliation ou sa résolution, tout litige ou différend issu d'un problème d'interprétation ou d'application de l'Entente, (ci-après désignés : « **différend** »), devront être soumis à l'arbitrage et ce, à l'exclusion des tribunaux, le tout, conformément à la procédure suivante.

Toute partie ayant un différend à faire valoir et désirant se prévaloir de l'arbitrage (ci-après désignée : la « **partie demanderesse** »), doit faire parvenir à l'autre partie (ou les autres Parties, selon le cas) un avis écrit (ci-après désigné : l'« **avis d'arbitrage** »), comportant les éléments suivants:

- Une description raisonnablement détaillée du différend soumis à l'arbitrage; et
- Le nom, l'adresse et la profession de la personne proposée pour agir comme arbitre unique.

L'autre partie (ou les autres Parties, selon le cas) doit, dans un délai de quinze (15) jours à compter de la réception de l'avis d'arbitrage, faire parvenir à la partie demanderesse un avis Écrit confirmant ou rejetant, selon le cas, le choix de l'arbitre proposé. À défaut par une partie de rejeter par Écrit le choix de l'arbitre suggéré par la partie demanderesse, elle sera réputée avoir accepté la nomination de l'arbitre proposé.

Dans le cas où une partie contestait le choix de l'arbitre, la partie la plus diligente pourra demander à un juge ayant juridiction de prendre toutes les mesures nécessaires pour assurer cette nomination conformément à l'article 625 du *Code de procédure civile*.

Les Parties s'engagent, avant de recourir aux dispositions qui suivent, à participer à au moins une (1) séance de conciliation avec l'arbitre. Cette séance doit se dérouler en français, à Montréal, entre le vingtième (20<sup>e</sup>) et le quarantième (40<sup>e</sup>) jours suivant la réception de l'avis d'arbitrage par la ou les autres Parties ou dans les quinze (15) jours suivant la nomination de l'arbitre unique par le tribunal.

L'arbitre pourra toutefois dispenser les Parties de la tenue de cette séance s'il juge, à son entière discrétion, que les circonstances ne s'y prêtent pas.

La tenue de séances de conciliation subséquentes nécessitera le consentement de toutes les Parties impliquées au différend et ce, nonobstant le deuxième alinéa de l'article 620 du *Code de procédure civile*. À défaut de tel consentement, l'arbitrage se poursuivra suivant les dispositions qui suivent.

L'arbitrage doit se dérouler en français, à Montréal.

L'audition des Parties au différend doit avoir lieu dans les vingt et un (21) jours suivant la date de la dernière séance de conciliation. L'arbitre aura le pouvoir de reporter, une seule fois et pour une période d'au plus trois (3) mois, la date d'audition pour tout motif qu'il jugera à propos, notamment, mais non limitativement, pour permettre à une partie de produire un rapport d'expert.

Nonobstant les dispositions de l'article 642 du *Code de procédure civile*, la sentence arbitrale doit être rendue dans les vingt et un (21) jours suivant la prise de délibéré. Toute sentence arbitrale ainsi rendue (incluant tout le processus de conciliation et d'arbitrage même) est strictement confidentielle et par conséquent, ne doit pas être divulguée à des tiers à moins qu'une telle divulgation ne soit requise par la loi, nécessaire à son homologation ou autrement nécessaire pour lui donner pleinement effet. Nonobstant les dispositions de l'article 637 du *Code de procédure civile*, les honoraires et frais d'arbitrage (incluant ceux se rapportant à la conciliation préalable) seront assumés entièrement par la partie qui succombera, sauf si, de l'avis de l'arbitre, ce résultat serait manifestement inéquitable dans les circonstances, auquel cas, ces honoraires et frais seront assumés en parts égales entre les Parties.

Les dispositions des articles 620 à 655 du *Code de procédure civile* compléteront le présent article et en cas de contradiction entre ces dispositions et celles du présent article, ces dernières auront préséance. Les règles relatives aux audiences et aux délais prévues aux articles 82 à 84 *Code de procédure civile* s'appliquent avec les adaptations nécessaires à l'arbitrage.

Toute référence au *Code de procédure civile* contenue au présent article constitue une référence au nouveau *Code de procédure civile*, RLRQ c C-25.01 dont l'entrée en vigueur de l'ensemble des dispositions est prévue au mois de janvier 2016 (incluant tout amendement pouvant lui être apporté de temps à autre).

Nonobstant la convention d'arbitrage qui précède, chaque partie pourra, en tout temps et à son entière discrétion, s'adresser à un tribunal plutôt qu'à un arbitre pour les matières suivantes, savoir :

- Injonction;
- Injonction interlocutoire;
- Injonction provisoire;
- Saisie avant jugement;
- Séquestre;
- Toute ordonnance de sauvegarde, notamment, mais non limitativement, l'ordonnance *Anton Piller*, l'ordonnance *Mareva* ou l'ordonnance *Norwich*.

Les matières énumérées ci-avant sont limitatives et toute autre matière devra donc être soumise à l'arbitrage, à l'exclusion des tribunaux.

Les Parties reconnaissent que de tels recours devant les tribunaux ont, contrairement à l'arbitrage, un caractère public. Les Parties conviennent de limiter les répercussions de ce caractère public et s'engagent à adopter toutes les mesures nécessaires pour limiter la diffusion aux tiers et au public en général de l'existence et des modalités de tels recours sauf dans la mesure où cela est requis par la loi ou nécessaire pour leur donner pleinement effet.

### **23. AVIS**

Tout avis en vertu des présentes doit être donné par Écrit et envoyé par toute mode approprié qui permet à celui qui l'envoie de constituer une preuve de la remise, de l'envoi, de la transmission ou de la publication du document. Ce sera par exemple le cas si un avis est envoyé par courrier recommandé à l'adresse du siège de la Partie concernée, tel que dénoncé de temps à autre au registraire des entreprises du Québec.

Les avis doivent toutefois être envoyés à l'attention des personnes suivantes :

Pour le Fournisseur : À l'attention de \*  
 Courriel : \* @\*

Pour la Chambre : À l'attention des Services juridiques et relations institutionnelles  
 Courriel : [servicesjuridiques@cnq.org](mailto:servicesjuridiques@cnq.org)

Pour l'Intervenante : À l'attention de \*  
 Courriel : \* @\*

### **24. EXEMPLAIRES**

Les Parties conviennent que l'original de l'Entente sera le document signé par toutes les Parties et conservé sur support « .pdf », le tout, à l'exclusion de tout document papier.

## 25. INTERVENTION

L'Intervenante, à titre de détentrice d'une licence générale pour le logiciel connu sous le nom de « \* » , déclare avoir eu communication des présentes, y donne son consentement à toutes fins que de droit, s'engage à se comporter de façon à donner plein effet aux présentes, accepte les stipulations faites en sa faveur et se déclare liée par les obligations la concernant, notamment, mais non limitativement, les obligations prévues à l'article 15.

De plus, l'Intervenante promet, d'une part, que tout nouveau Fournisseur désigné par elle aux termes de l'article 15 adhèrera à la présente Entente ou à toute autre version alors en vigueur et, d'autre part, que tout nouveau Fournisseur ainsi désigné assumera toutes les obligations non remplies aux termes de la présente Entente par le Fournisseur actuel ou tout autre Fournisseur désigné par l'Intervenante, le cas échéant.

Les promesses de l'Intervenante dans le cadre du présent article constituent des promesses du fait d'autrui au sens du *Code civil du Québec*.

**EN FOI DE QUOI**, les Parties ont signé aux dates indiquées ci-dessous :

À Montréal, le \* [Date de signature]

**CHAMBRE DES NOTAIRES DU QUÉBEC**

---

Par : M<sup>e</sup> Stéphane BRUNELLE, directeur général

À \* [Ville], le \* [Date de signature]

\* [NOM DU FOURNISSEUR]

---

Par : \* [Nom du représentant du fournisseur]

À \* [Ville], le \* [Date de signature]

\* [NOM DE L'INTERVENANTE]

---

Par : \* [Nom du représentant de l'Intervenante]

**Annexe à l'Entente de fourniture de service d'externalisation aux notaires  
entre  
\* [Nom du fournisseur] et la Chambre des notaires du Québec**

Le contenu de cette annexe doit faire partie du Contrat de service Écrit conclu entre le Fournisseur et chaque Notaire avec qui il fait affaire au sens de l'article 7 de l'Entente de fourniture de service d'externalisation aux notaires. Les dispositions de cette annexe ont préséance sur toute disposition contractuelle contraire ou inconciliable contenue dans tout autre contrat conclu entre le Fournisseur et le Notaire (incluant ici tout contrat conclu avec toute société par l'entremise de laquelle le Notaire exerce sa profession, le cas échéant).

De plus, les dispositions de cette annexe ne doivent pas être interprétées comme venant diminuer ou autrement alléger les obligations du Notaire aux termes de la loi, notamment, mais non limitativement, celles prévues au *Règlement sur la tenue des dossiers et des études des notaires* et au *Règlement sur la comptabilité en fidéicommiss des notaires*.

## **1. DÉFINITIONS**

Les mots et expressions qui suivent ont, sauf si le contexte le requiert autrement, le sens qui leur est ci-après donné et ce, indépendamment du fait qu'ils débutent ou non par une lettre majuscule :

### **1.1 « Ayant droit »**

signifie toute personne ayant le pouvoir d'exercer un droit sur les Documents technologiques en vertu du *Code des professions*, de la *Loi sur le notariat* applicable et des règlements qui en découlent, notamment le syndic ou le secrétaire de la Chambre.

### **1.2 « Chambre »**

désigne la CHAMBRE DES NOTAIRES DU QUÉBEC, personne morale de droit public régie par le *Code des professions* et par la *Loi sur le notariat*, inscrite au fichier des autorités publiques sous le numéro 8814180590, ayant son siège au 2045, rue Stanley, suite 101, Montréal, province de Québec, H3A 2V4.

### **1.3 « Contrat » ou « Contrat de service »**

signifie le présent contrat de fourniture de service conclu entre le Fournisseur et le Notaire, \* lequel prend la forme d'une licence d'utilisation.

#### **1.4 « Directive de sécurité »**

signifie la « *Directive de sécurité - Fournisseurs de service d'externalisation aux notaires* » adoptée par la Chambre et en vigueur au moment de la signature du présent Contrat ainsi que chaque modification qui y sera apportée unilatéralement par la Chambre. Cette directive de sécurité régit le cadre de la sécurité des Documents technologiques et de leur accès, tant sur le plan administratif, technique que physique, sauf si le Fournisseur est certifié ou se soumet volontairement au respect d'une Norme plus sévère et contraignante, auquel cas, cette dernière a préséance sur la Directive de sécurité.

#### **1.5 « Document technologique »**

signifie un document échangé, généré, produit, conservé ou transmis par un Notaire de quelque manière qu'il soit et dont le support fait appel aux technologies de l'information, au sens de la *Loi concernant le cadre juridique des technologies de l'information*, incluant toutes données, banques de données et métadonnées sous-jacentes qui en permettent la création. À titre d'exemple, il peut s'agir de Renseignements confidentiels, de renseignements personnels au sens des lois applicables en l'espèce, d'informations sur les clients, de courriels, de contrats ou d'ébauches d'avis juridique. Le Document technologique appartient au Notaire.

#### **1.6 « Écrit »**

désigne tout écrit porté sur quelque support ou technologie que ce soit, le tout en conformité avec la liberté prévue à cet effet à l'article 2 de la *Loi concernant le cadre juridique des technologies de l'information*.

#### **1.7 « Entente de fourniture de service d'externalisation »**

signifie l'entente de fourniture de service d'externalisation aux notaires intervenue entre la Chambre et le Fournisseur, incluant son préambule, chaque document annexé à celle-ci et chaque modification ou ajout qui lui est apporté dans le temps.

#### **1.8 « Force majeure »**

signifie l'intervention d'un événement extérieur, irrésistible et imprévisible, telle qu'une catastrophe naturelle, et qui empêche l'exécution d'une obligation.

### **1.9 « Fournisseur »**

signifie la personne morale comparaisant au présent Contrat

### **1.10 « Norme »**

Signifie une norme plus sévère et plus contraignante que la Directive de sécurité, en matière de gouvernance et de sécurité des technologies de l'information, élaborée et mise à jour régulièrement par un organisme international compétent et reconnu par la Chambre, à laquelle le Fournisseur se soumet volontairement ou pour laquelle il détient une certification.

### **1.11 « Notaire »**

signifie la personne titulaire d'un permis d'exercice délivré par la Chambre, inscrite ou non au tableau de l'Ordre, qui utilise le Service d'externalisation et qui est partie au présent Contrat, excluant la société au sein de laquelle un notaire exerce ses activités professionnelles.

### **1.12 « Nouveau service proposé »**

désigne toute nouvelle caractéristique ou fonctionnalité importante, tout logiciel, toute application ou tout service que le Fournisseur se propose d'incorporer au Service d'externalisation. Pour plus de précision, une simple amélioration des caractéristiques ou fonctionnalités du Service d'externalisation ne constitue pas un Nouveau service proposé.

### **1.13 « Partenaire »**

signifie indistinctement tout mandataire, sous-traitant, consultant, partenaire d'affaires, revendeur, prestataire de services ou entrepreneur du Fournisseur, ainsi que les partenaires de ces derniers.

### **1.14 « Renseignement confidentiel »**

signifie une information reçue par l'une des parties au Contrat, sous quelque forme et de quelque façon que ce soit, qui concerne l'une des parties ou tout Notaire, ses employés, ses activités, ses produits ou ses procédés, sa clientèle ou ses fournisseurs et qui est désignée par l'une des parties comme étant confidentielle ou qui doit être considérée comme étant confidentielle selon sa nature et les circonstances de la divulgation, incluant toute information sujette au secret professionnel.

### **1.15 « Service d'externalisation »**

signifie un service offert par un Fournisseur permettant à un Notaire de transférer ou de confier, peu importe le moyen, en tout ou en partie, ses Documents technologiques et ses ressources informatiques physiques ou logicielles. Ce service peut notamment être la sauvegarde des Documents technologiques à distance, l'hébergement d'équipements informatiques, l'exploitation d'un système d'information ou d'applications.

Dans le cas du Fournisseur, le « Service d'externalisation » consiste en un logiciel de \*, connu sous le nom de « \* ».

Toutefois, « Service d'externalisation » ne désigne pas \*.

Enfin, « Service d'externalisation » désigne tout Nouveau service proposé.

## **2. RÈGLES D'INTERPRÉTATION**

### **2.1 Lois applicables**

Le Contrat est régi et interprété selon les lois en vigueur dans la province de Québec.

### **2.2 Délais de rigueur**

Tous les délais prévus au Contrat sont de rigueur.

### **2.3 Absence de stipulation pour autrui**

Le présent Contrat ne doit en aucun cas être interprété comme contenant une ou des stipulations pour autrui qui seraient faites en faveur de clients de Notaires.

## **3. ENGAGEMENTS ET CONSENTEMENTS DU FOURNISSEUR**

### **3.1 Prestation du Service d'externalisation**

Le Fournisseur s'engage :

- à fournir le Service conformément à la plus récente Entente de fourniture de service d'externalisation, à la Norme et à la Directive de sécurité et en respectant les engagements pris auprès de la Chambre concernant la prestation du Service d'externalisation, notamment, mais non limitativement, ceux décrits au Contrat;



- à maintenir le Service d'externalisation de façon continue et ininterrompue pendant toute la durée du Contrat, le tout, sous réserve de ce qui suit : le Fournisseur doit assurer la disponibilité des Documents technologiques en moins de soixante-douze (72) heures en cas de Force majeure. Si le Service d'externalisation devait être interrompu durant les heures normales de bureau du Notaire pour des raisons ne relevant pas de la Force majeure ou d'un entretien planifié, le Fournisseur devra faire en sorte que le Service d'externalisation soit rétabli au plus tard quatre (4) heures consécutives non entrecoupées d'un jour de congé, à compter de l'interruption;
- à aviser préalablement le Notaire de la tenue de tout entretien planifié, de mise à niveau ou de toute autre opération du genre qui auront pour effet de rendre le Service d'externalisation indisponible;
- à rendre disponible au Notaire, sur simple demande verbale de sa part ou de l'initiative du Fournisseur, un service de soutien technique et tout autre service connexe permettant d'assurer le maintien des opérations professionnelles du Notaire.

### **3.2 Accessibilité aux Documents technologiques**

Le Fournisseur s'engage à rendre les Documents technologiques accessibles en tout temps (sous réserve des dispositions de l'article 3.1) au Notaire ou aux Ayants droit, sur leur simple demande verbale.

### **3.3 Remise des Documents technologiques par le Fournisseur**

Le Fournisseur doit remettre les Documents technologiques à l'une ou l'autre des personnes suivantes, selon les circonstances ci-après décrites :

- a) au Notaire ou aux Ayants droit, selon le cas, lors de la résiliation du Contrat de service, sur simple demande;
- b) à un nouveau Fournisseur désigné par le Notaire ou par les Ayants droit lors de la résiliation du Contrat de service, sur simple demande et, dans le cas des Ayants droit, sur justification de leur titre;
- c) si le Fournisseur cesse d'offrir le Service d'externalisation pour quelque raison que ce soit sans qu'un autre fournisseur ne poursuive son exploitation \* ou ne soit désigné par l'Intervenante conformément à l'article 15 de l'Entente immédiatement après cette cessation conformément aux dispositions des présentes, au fournisseur désigné par la Chambre sur demande de son secrétaire;

- d) à toute personne autorisée par la loi ou par la Chambre, notamment au syndic de la Chambre, à recevoir ces Documents technologiques en vertu de la loi et des règlements qui régissent la profession notariale, sur simple demande.

Pour plus de précision, une telle demande peut être effectuée après la résiliation de l'Entente de fourniture de service d'externalisation, sujet toutefois à la destruction des Documents technologiques prévue ci-après.

L'intégralité des Documents technologiques en possession du Fournisseur doit, dans tous les cas, être remise de façon sécuritaire et au plus tard dans un délai de quinze (15) jours de la demande. Le Fournisseur qui souhaite facturer quelques frais ou honoraires que ce soit au Notaire relativement à la remise des Documents technologiques de ce dernier ne peut en exiger le paiement tant que cette remise n'est pas entièrement complétée.

### **3.4 Destruction des Documents technologiques par le Fournisseur**

Le Fournisseur doit détruire tous les exemplaires de Documents technologiques (en production, redondance et sauvegarde) de façon sécuritaire, de la manière prévue à la Norme et à la Directive de sécurité, peu importe le support sur lequel ils se trouvent, en fonction de ce qui est prévu au présent article.

Le Fournisseur ne peut détruire les Documents technologiques avant d'avoir transmis au Notaire au préavis Écrit de 60 jours lui précisant la marche à suivre afin de les récupérer.

Le Fournisseur doit détruire tous les Documents technologiques d'un Notaire au plus tard 120 jours après la réception par le Notaire de ce préavis Écrit.

## **4. DÉFENSE ET INDEMNISATION**

Le Fournisseur reconnaît que le Notaire ne peut être tenu responsable des dommages ou pertes attribuables à des droits de propriété intellectuelle de Partenaires ou de tiers et dégage le Notaire de toute responsabilité à cet égard, directe ou indirecte.

Le Fournisseur doit défendre et indemniser le Notaire et le dégager de toute responsabilité à l'égard de toute réclamation d'une tierce partie intentée contre lui, dans la mesure où cette réclamation : (i) découle d'une violation à des droits de propriété intellectuelle; ou (ii) découle d'un manquement du Fournisseur à ses obligations relatives à la sécurité de l'information (disponibilité, confidentialité et intégrité).

Le Fournisseur ne peut limiter sa responsabilité découlant d'une violation à des droits de propriété intellectuelle et d'un manquement du Fournisseur à ses obligations relatives à la sécurité de l'information.

Cet engagement du Fournisseur n'est valable qu'à condition que le Notaire informe le Fournisseur par Écrit de la réclamation en question, dans les quinze (15) jours ouvrables de sa connaissance, qu'il laisse au Fournisseur la maîtrise exclusive de la défense dans le cadre de ladite réclamation et de toute négociation connexe visant la conclusion d'un règlement à l'amiable, qu'il coopère avec le Fournisseur, et qu'il aide ce dernier, à sa demande et à ses frais, à mener à bien cette défense.

Le Fournisseur pourra conclure un règlement à l'amiable à l'égard de toute réclamation qui est couverte par l'indemnité offerte aux termes de cet article sans l'approbation du Notaire, dans la mesure où ce règlement n'implique pas ou ne suggère pas une admission de responsabilité de la part du Notaire.

## **5. MOTIFS DE RÉSILIATION**

En plus de tous autres motifs convenus entre le Notaire et le Fournisseur, ceux-ci conviennent que la résiliation de l'Entente de fourniture de service d'externalisation emportera résiliation du Contrat. À cet effet, le Fournisseur aura l'obligation d'aviser le Notaire sans délai de la survenance d'une telle résiliation.

## **6. CONFIDENTIALITÉ DE L'INFORMATION**

Le Fournisseur s'engage à :

- ce que ni lui, ses employés, agents, Partenaires, représentants ou dirigeants n'utilisent ou ne divulguent un Renseignement confidentiel à l'égard du Notaire et/ou de ses clients sans y être dûment et expressément autorisé par les personnes habilitées à le faire;
- respecter la loi applicable au Québec relativement à tout Renseignement confidentiel.

Le Fournisseur se porte garant du non-respect de tout engagement le concernant par ses employés, agents, Partenaires, représentants ou dirigeants et consent à assumer l'entière responsabilité de tout dommage pouvant découler du non-respect du caractère confidentiel des Renseignements confidentiels en possession de ces personnes.

Le Fournisseur doit assurer la protection des Documents technologiques des Notaires et ne pas se comporter de façon à violer le secret professionnel du Notaire se rapportant à ces Documents technologiques, notamment, en informant des tiers du nom de clients de Notaires, sauf du

consentement du client concerné.

Le Fournisseur doit assurer la protection des Documents technologiques contre les accès non autorisés et ne pas les utiliser à d'autres fins que celles faisant l'objet du Contrat.

## **7. SECRET PROFESSIONNEL**

Le Fournisseur reconnaît expressément que de nombreux Documents technologiques qui lui sont transmis, dans le cadre du Service d'externalisation, sont protégés par le secret professionnel du Notaire.

Le Fournisseur reconnaît que ce secret professionnel est un principe fondamental dans notre droit et tire sa source de divers lois et règlements, notamment, mais non limitativement, les suivants:

- *Charte des droits et libertés de la personne*, RLRQ, c. C-12, art. 9;
- *Loi sur le notariat*, RLRQ, c. N-3, art. 14.1;
- *Règlement sur la comptabilité en fidéicommiss des notaires*, RLRQ, c. N-3, r. 5.2, art. 3 et 33
- *Code de déontologie des notaires*, RLRQ, c. N-3, r. 2.

Par conséquent, le Fournisseur s'engage à :

- Se comporter de façon à protéger le secret professionnel des Documents technologiques qui lui sont transmis par le Notaire;
- Limiter l'accès aux Documents technologiques protégés par le secret professionnel aux personnes qui doivent absolument y avoir accès, les informer du fait que les Documents technologiques sont ainsi protégés par le secret professionnel et leur faire souscrire un engagement Écrit à se comporter de façon à protéger le secret professionnel de ces Documents technologiques;
- Aviser sans délai le Notaire de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité (incluant les dispositions de l'article précédent) et relatives à la protection du secret professionnel et ce, tant à l'égard de violations contractuelles que de celles qui pourraient découler de l'application d'une loi, notamment, mais non limitativement, de toutes lois fiscales. Cette disposition a préséance sur toute autre disposition.

Le présent article ne doit en aucun temps être interprété comme limitant ou restreignant la portée générale des autres dispositions du Contrat, notamment, des dispositions de l'article précédent.

## **8. ASSURANCES**

Le Fournisseur doit souscrire et maintenir en vigueur pendant la durée de l'Entente, à ses frais et auprès de compagnies d'assurance reconnues, des polices d'assurance des types et pour les montants de couverture ci-après mentionnés comportant des franchises d'un montant maximum de DIX MILLE DOLLARS (10 000 \$) :

- 8.1** Assurance générale d'entreprise sur les biens couvrant le contenu et les biens matériels qui sont affectés à la prestation du Service d'externalisation pour garantir les pertes et les dommages causés par le feu, l'eau, le vol et le vandalisme pour le plein montant de la valeur de remplacement des biens.
- 8.2** Assurance responsabilité civile qui doit avoir une limite minimale de deux millions de dollars (2 000 000 \$) par sinistre.
- 8.3** Assurance offrant une couverture cyber-risques couvrant minimalement :
  - La responsabilité pour des atteintes à la sécurité des réseaux informatiques, de l'information et de la confidentialité des renseignements personnels;
  - La protection des actifs informationnels ou produits technologiques;
  - Le remboursement des frais liés à la gestion des incidents affectant la sécurité des réseaux informatiques, l'information et la confidentialité des renseignements personnels, incluant les services professionnels et technologiques des tiers;
  - Les frais de défense, les frais d'enquête et une garantie à l'encontre des pénalités administratives;
  - La cyber-extorsion.

Chacune des garanties mentionnées à l'article 8.3 devant faire état d'une limite de deux millions de dollars (2 000 000 \$) par sinistre et de cinq millions de dollars (5 000 000 \$) par période annuelle.

## **9. ENGAGEMENTS ET DÉCLARATIONS DU NOTAIRE**

Le Notaire s'engage envers la Chambre, laquelle accepte cet engagement en sa faveur, à respecter la résiliation de l'Entente de fourniture de service d'externalisation, le tout, sans possibilité d'exiger de dommages-intérêts de la Chambre ou quelque autre compensation que ce soit à son égard ou d'intenter à l'égard de la Chambre quelque recours que ce soit.

Par ailleurs, le Notaire reconnaît que la Chambre n'effectue pas un audit complet des activités du Fournisseur et qu'à ce titre, divers éléments, notamment, mais non limitativement, la performance globale du Service d'externalisation, les fonctionnalités du Service d'externalisation et la qualité du service à la clientèle du Fournisseur ne font pas l'objet d'une évaluation ou d'un contrôle par la Chambre. Par conséquent, il est de la responsabilité du Notaire de s'assurer que ces éléments conviennent à ses besoins.

Le Notaire reconnaît que la Chambre ne peut être tenue responsable des manquements du Fournisseur aux obligations qui lui incombent.

Le Notaire s'engage à aviser la Chambre dans les quinze (15) jours ouvrables de sa connaissance d'une réclamation d'un tiers découlant des motifs prévus à l'article 4 du présent Contrat de service.

## **10. MODIFICATIONS AU CONTRAT**

Le Fournisseur s'engage à modifier le Contrat pour y intégrer toute modification apportée par l'Entente de fourniture de service d'externalisation et à y faire adhérer les Notaires, dans les quatre-vingt-dix (90) jours de telle modification.

## **11. SURVIE DES OBLIGATIONS**

Les obligations du Fournisseur prévues aux articles indiqués ci-après entre parenthèses survivent à la fin du présent Contrat de service pour la durée indiquée :

- 11.1** Sécurité, protection, destruction des Documents technologiques (articles 3.1, 6 et 7) : les obligations du Fournisseur envers le Notaire s'éteindront une fois survenue la destruction prévue à l'article 3.4.
- 11.2** Confidentialité, secret professionnel (articles 6 et 7) : les obligations du Fournisseur survivent perpétuellement.
- 11.3** Défense et indemnisation (article 4): les obligations du Fournisseur s'éteindront à l'expiration d'un délai de trois (3) ans suivant la date de fin du Contrat de service.
- 11.4** Assurances (article 8) : les obligations du Fournisseur s'éteindront à l'expiration d'un délai de trois (3) ans suivant la date de fin du Contrat de service.

## **12. ENTRÉE EN VIGUEUR**

La présente annexe entre en vigueur à la plus rapprochée de la date de la clôture du Contrat ou à la date d'entrée en vigueur d'une entente conclue entre le Fournisseur et la Chambre autorisant le Fournisseur à conclure ce Contrat de service.

À TITRE INDICATIF SEULEMENT

## Directive de sécurité

---

### Fournisseurs de service d'externalisation aux notaires

*Préparé et sous la responsabilité du Secrétariat de l'Ordre  
Approuvé le : 20 février 2014 à la séance du Comité exécutif  
Mis à jour le : 18 novembre 2015 à la séance du Comité exécutif  
Modifié le : 22 juin 2016 par le Secrétariat de l'Ordre dans les limites de ses pouvoirs  
Responsable : Danielle Gagliardi, Secrétaire de l'Ordre*



## Table des matières

1. Domaine d'application.....	4
2. Termes et définitions.....	4
3. Politique de sécurité.....	5
3.1 Politique de sécurité de l'information .....	5
4. Contrat de service.....	6
5. Gestion des biens .....	7
5.1 Responsabilités relatives aux Actifs informationnels.....	7
5.2 Classification des informations .....	7
6. Sécurité liée aux ressources humaines.....	7
6.1 Avant le recrutement .....	7
6.2 Pendant la durée du contrat d'embauche .....	8
6.3 Fin ou modification de contrat d'embauche .....	8
7. Sécurité physique et environnementale .....	8
7.1 Zones sécurisées .....	8
7.2 Sécurité du matériel.....	9
8. Gestion de l'exploitation et des télécommunications .....	9
8.1 Procédures et responsabilités liées à l'exploitation .....	9
8.2 Sauvegarde.....	9
8.3 Gestion de la sécurité des réseaux.....	10
8.4 Manipulation des supports.....	10
8.5 Échange des informations .....	11
8.6 Service de commerce électronique.....	11
8.7 Surveillance.....	11
9. Contrôle d'accès du personnel du Fournisseur .....	11
9.1 Gestion de l'accès utilisateur .....	11
9.2 Responsabilités utilisateurs .....	12
9.3 Contrôle d'accès au réseau .....	12
9.4 Contrôle d'accès aux applications et à l'information.....	13
9.5 Informatique mobile et télétravail .....	13
10. Développement et maintenance des systèmes .....	13
10.1 Bon fonctionnement des applications .....	13
10.2 Mesures cryptographiques .....	13
10.3 Sécurité des fichiers système .....	14
10.4 Sécurité en matière de développement et d'assistance technique.....	14
10.5 Gestion des vulnérabilités techniques .....	14
11. Gestion des Incidents liés à la sécurité de l'information .....	14
11.1 Signalement des événements et des failles liés à la sécurité de l'information. 14	
12. Gestion du plan de continuité de l'activité .....	15
12.1 Aspects de la sécurité en matière de gestion de la continuité de l'activité .....	15

13.	Remise des Actifs informationnels aux notaires .....	16
14.	Destruction sécuritaire des Documents technologiques .....	16
15.	Signature numérique des notaires .....	16

## 1. Domaine d'application

La présente Directive établit des lignes directrices et des principes généraux concernant les services d'externalisation offerts aux notaires. Les objectifs présentés dans la présente Directive fournissent une orientation générale sur ce qui est communément accepté dans la gestion de la sécurité de l'information.

Les objectifs et mesures sont destinés à être mis en œuvre pour répondre aux exigences identifiées. La présente Directive représente une base commune et donne des lignes directrices pratiques pour élaborer les référentiels de sécurité, mettre en œuvre les pratiques efficaces de la gestion de la sécurité et développer un environnement de confiance dans les activités des fournisseurs.

La présente Directive de sécurité s'applique à tous les Fournisseurs de Service d'externalisation. Les mesures et contrôles applicables doivent tenir compte du service offert par le Fournisseur.

## 2. Termes et définitions

Pour les besoins du présent document, les mots et expressions qui suivent ont, sauf si le contexte le requiert autrement, le sens qui leur est ci-après donné et ce, indépendamment du fait qu'ils débutent ou non par une lettre majuscule :

### **Actif informationnel**

Les actifs informationnels visés par la présente Directive comprennent les Documents technologiques, les liens de communication, les sites d'hébergement et les équipements relatifs à l'exploitation du Service d'externalisation.

### **Contrat de service**

Signifie le contrat de fourniture de service d'externalisation aux notaires que le Fournisseur doit conclure avec le notaire selon les modalités de l'*Entente de fourniture de service d'externalisation aux notaires* conclue avec la Chambre des notaires. Le contrat de service est constitué d'un écrit contenant minimalement les dispositions de l'Annexe de cette Entente.

### **Document technologique**

Signifie un document transmis par un notaire de quelque manière qu'il soit et dont le support fait appel aux technologies de l'information, au sens de la *Loi concernant le cadre juridique des technologies de l'information*, incluant toutes données, banques de données et métadonnées sous-jacentes qui en permettent la création. À titre d'exemple, il peut s'agir de Renseignements confidentiels, de renseignements personnels au sens des lois applicables en l'espèce, d'informations sur les clients, de courriels, de contrats ou d'ébauches d'avis juridique. Le Document technologique appartient au notaire.

### **Force majeure**

Intervention d'un événement extérieur, irrésistible et imprévisible, telle qu'une catastrophe naturelle, et qui empêche l'exécution d'une obligation.

### **Fournisseur**

Entreprise externe, incluant ses Partenaires, qui offre un Service d'externalisation aux notaires et qui est autorisé par la Chambre des notaires.

### **Incident lié à la sécurité de l'information**

Un incident lié à la sécurité de l'information découle d'un ou plusieurs événements(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre

les opérations liées à l'activité du Fournisseur et de menacer la sécurité de l'information de ses clients notaires.

**Interruption**

Toute indisponibilité temporaire d'un Actif informationnel, à l'exception de celle résultant d'une Force majeure.

**Partenaire**

Signifie indistinctement tout mandataire, sous-traitant, consultant, partenaire d'affaires, revendeur, prestataire de services ou entrepreneur du Fournisseur, ainsi que les partenaires de ces derniers.

**Renseignement confidentiel**

Signifie une information reçue, sous quelque forme et de quelque façon que ce soit, qui concerne le Fournisseur ou tout notaire, ses employés, ses activités, ses produits ou ses procédés, sa clientèle ou ses fournisseurs et qui est désignée comme étant confidentielle ou qui doit être considérée comme étant confidentielle selon sa nature et les circonstances de la divulgation, incluant toute information sujette au secret professionnel.

**Service d'externalisation**

Signifie un service offert par un Fournisseur permettant à un notaire de transférer ou de confier, peu importe le moyen, en tout ou en partie, ses Documents technologiques et ses ressources informatiques physiques ou logicielles. Ce service peut notamment être la sauvegarde des Documents technologiques à distance, l'hébergement d'équipements informatiques, l'exploitation d'un système d'information ou d'applications.

### 3. Politique de sécurité

#### 3.1 Politique de sécurité de l'information

*« Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. »*

Le Fournisseur doit avoir une politique de sécurité de l'information approuvée et endossée par la direction de son entreprise. Cette politique doit être communiquée, publiée et endossée par les employés du Fournisseur.

La politique de sécurité du Fournisseur doit faire partie de sa politique générale et doit être revue périodiquement avec tous les documents auxquels elle fait référence afin de s'assurer qu'elle soit à jour et alignée aux objectifs et stratégies du Fournisseur.

Le document de politique de sécurité de l'information doit inclure au minimum:

- Une définition de la sécurité de l'information, ses objectifs et sa portée;
- Une déclaration des intentions de la direction du Fournisseur soutenant les objectifs et principes de la sécurité de l'information, en conformité avec la stratégie et les objectifs du Fournisseur;
- Une démarche de définition des objectifs de sécurité et des mesures, intégrant l'appréciation et la gestion du risque;
- Une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour le Fournisseur, à savoir les éléments suivants:
  - la conformité avec les exigences légales, réglementaires et contractuelles;

- la gestion de la continuité de l'activité;
- une liste des contrôles et des objectifs qu'ils sous-tendent;
- un programme d'éducation et de sensibilisation.
- Une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'Incidents liés à la sécurité de l'information, ainsi que les conséquences aux manquements et sanctions applicables;
- Les références à toute documentation susceptible d'appuyer la politique et devant être respectée.

Référence: ISO27001:2013 A-5.2

#### 4. Contrat de service

En plus des conditions prévues à l'*Entente de fourniture de service d'externalisation aux notaires*, le Fournisseur doit utiliser une entente de confidentialité et de non-divulgaration, laquelle doit refléter ses besoins et ceux de ses clients notaires en matière de protection de l'information. Cette entente doit être revue périodiquement et doit minimalement adresser les points suivants:

- Une définition de l'information à protéger;
- La durée de l'entente;
- Les conséquences aux manquements et sanctions applicables à une divulgation non autorisée de l'information;
- Les droits et limites d'utilisation relative à l'information;
- Le processus général pour la notification d'un manquement à l'entente de confidentialité ou tout autre incident majeur, entre autres:
  - 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.
- Les conditions pour le transfert ou la destruction de l'information à la fin de l'entente contractuelle avec ses clients notaires;
- La conformité aux différentes lois et aux règles régissant la profession notariale ainsi que le respect des droits des personnes concernées par les Documents technologiques.

Référence: ISO27001:2013 A-15.

#### Tiers

« Assurer la sécurité de l'information et des moyens de traitement de l'information consultés, opérés, communiqués ou gérés par des tiers. »

La présente Directive s'applique aux tiers concernés et ils doivent s'y conformer. Par conséquent, si le Fournisseur sous-traite totalement ou en partie ses services à un Partenaire, c'est au Fournisseur de s'assurer que ce dernier respecte en tout point la Directive et de lui faire signer une entente à cet effet. Cette entente doit être conforme aux engagements pris par le Fournisseur avec la Chambre des notaires ainsi qu'avec ses clients notaires.

Le Fournisseur est imputable du Service d'externalisation et par conséquent, il est responsable de toutes les actions de ses Partenaires. Le Fournisseur doit déclarer ses Partenaires à la Chambre des notaires en tout temps et déclarer s'il est propriétaire ou non :

- (i) des Actifs informationnels par lesquels sont transférés, conservés, copiés et généralement traités les Documents technologiques;
- (ii) des locaux dans lesquels sont situés les Actifs informationnels; et
- (iii) du Service d'externalisation et des solutions qui le composent et qui permettent de l'offrir.

Référence: ISO27001:2013

## 5. Gestion des biens

### 5.1 Responsabilités relatives aux Actifs informationnels

« *Mettre en place et maintenir une protection appropriée des biens de l'organisme.* »

Afin de maintenir la protection des Actifs informationnels relatifs à la Directive, chaque actif doit être répertorié et assigné à un propriétaire qui aura la responsabilité de maintenir les contrôles appropriés afin d'en assurer sa protection.

Les Actifs informationnels doivent demeurer au Canada et, en aucun temps, ne doivent transiter, être sauvegardés ou être traités à l'extérieur du Canada. Il est de la responsabilité du Fournisseur de s'assurer que cette obligation est respectée en tout temps.

Les Actifs informationnels doivent être utilisés, communiqués, protégés et/ou détruits en respect avec la présente Directive ainsi que les politiques applicables du Fournisseur.

Référence: ISO27001:2013

### 5.2 Classification des informations

« *Le fournisseur convient de garantir un niveau de protection approprié aux informations.* »

Afin de s'assurer que les Documents technologiques sont protégés adéquatement, ceux-ci doivent être classifiés en termes de confidentialité, d'intégrité et/ou de disponibilité. Un système de classification doit être mis en place et les Documents technologiques faisant l'objet du Service d'externalisation doivent être classifiés selon le plus haut niveau dans l'échelle.

Exemple :

Niveau de classification	Information
Confidentiel	Documents technologiques, etc.
Interne	Documentation des systèmes, etc.
Public	Site Web corporatif, etc.

Le Fournisseur doit individualiser et séparer les Documents technologiques de chacun de ses clients notaires afin d'en protéger la confidentialité et d'en faciliter la recherche, le transfert et la récupération lorsque requis.

Référence: ISO27001:2013

## 6. Sécurité liée aux ressources humaines

### 6.1 Avant le recrutement

« *Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées à réduire le risque de vol, de fraude*

*ou de mauvais usage des équipements. Il convient de sélectionner avec soin tous les postulants, contractants et utilisateurs tiers, surtout lorsqu'il s'agit de tâches critiques. »*

Les employés et Partenaires du Fournisseur, ou toutes autres personnes qu'il autorise, impliqués dans le Service d'externalisation, doivent subir une enquête de sécurité, incluant notamment, une vérification des références ainsi que des antécédents judiciaires.

Le contrat d'embauche doit spécifier les règles de confidentialité et de non-divulgence à respecter.

Référence: ISO27001:2013 A-7.1.

## **6.2 Pendant la durée du contrat d'embauche**

Le contrat d'embauche doit spécifier que l'employé doit informer le Fournisseur de toutes situations pouvant modifier les conclusions de son enquête de sécurité. Le contrat d'embauche doit également spécifier que l'enquête de sécurité peut être renouvelée annuellement ou à la discrétion du Fournisseur.

Il est de la responsabilité du Fournisseur de faire, au minimum à tous les deux ans, une mise à jour des enquêtes de sécurité de ses employés ou des autres personnes autorisées à intervenir dans les activités de support du Service d'externalisation.

## **6.3 Fin ou modification de contrat d'embauche**

*« Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie. »*

Le Fournisseur doit avoir une procédure formelle pour la restitution des biens, la modification ou la suppression des droits d'accès aux moyens de traitement de l'information lors de la fin ou de la modification du contrat d'embauche d'un de ses employés.

Référence: ISO27001:2013 A-7.3.

# **7. Sécurité physique et environnementale**

## **7.1 Zones sécurisées**

*« Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et les informations de l'organisme. »*

Les Actifs informationnels doivent être protégés par des mesures de sécurité physique permettant le contrôle des accès aux employés autorisés seulement.

Les exigences en matière de sécurité physique pour la salle d'hébergement sont:

- Les murs doivent être renforcés allant du vrai plancher au vrai plafond;
- Les portes d'accès ou de sortie d'urgence doivent être pleines;
- Pour une salle d'hébergement située à un niveau inférieur au troisième étage, les vitres extérieures devraient être obstruées par un grillage ou tout autre moyen dissuasif;
- Un système de contrôle d'accès ou poste de garde avec vérification d'identité doit être en place;
- Un registre des accès (nom, date, heure d'entrée et de sortie) doit être en place;
- La salle d'hébergement doit être pourvue d'un système de surveillance ou, lorsque la surveillance n'est pas possible, d'un système de détection d'intrusion actif en l'absence d'une personne autorisée;

- L'accès à la salle d'hébergement ne doit être possible qu'à partir d'une autre zone à accès contrôlé et non depuis une zone à accès public;
- Le personnel non autorisé à la salle d'hébergement doit être accompagné d'un garde ou d'un membre du personnel autorisé.

Référence: ISO27001:2013 A-11

## 7.2 Sécurité du matériel

« Empêcher la perte, l'endommagement, le vol ou la compromission des biens et l'interruption des activités de l'organisme. »

Les exigences en matière de sécurité matérielle applicables sont:

### Salle d'hébergement

- La salle d'hébergement doit être dotée d'une alimentation électrique d'appoint conforme aux normes de protection contre les incendies;
- La climatisation de la salle d'hébergement doit être suffisante aux besoins des équipements s'y trouvant et conforme aux normes de protection contre les incendies;
- La température et l'humidité doivent être contrôlées;
- Si l'information n'est pas chiffrée, le câblage réseau ne devrait pas passer dans une zone publique.
- Les mesures de protection contre les incendies doivent être égales ou supérieures aux meilleures pratiques de l'industrie du Service d'externalisation.

### Cabinets

- Les cabinets contenant les serveurs hébergeant des Renseignements confidentiels doivent être verrouillés;
- L'accès aux cabinets doit être restreint au personnel autorisé seulement.

Référence: ISO27001:2013 A-11

## 8. Gestion de l'exploitation et des télécommunications

### 8.1 Procédures et responsabilités liées à l'exploitation

« Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information. »

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

Référence: ISO27001:2013 A-12

### 8.2 Sauvegarde

« Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information. »

La sauvegarde des Documents technologiques doit être faite quotidiennement et doit être chiffrée. Des tests de restauration concluants doivent être exécutés au minimum une fois par mois.

La sauvegarde des Documents technologiques ne peut être faite à l'extérieur du Canada.

Dans le cas d'un Service d'externalisation d'hébergement d'infrastructure ou d'applications, une copie de sauvegarde des Documents technologiques doit être entreposée à l'extérieur de



l'immeuble du Fournisseur, mais en territoire canadien, au moins une fois par semaine, dans des locaux répondant aux exigences de sécurité décrites à la présente Directive.

Les archives et les sauvegardes, peu importe le support, doivent faire l'objet d'une procédure claire quant à leur identification et manipulation. Cette information est importante et confidentielle et ne devrait être manipulée, détenue et/ou détruite que par le personnel ou les parties autorisées.

Le Fournisseur doit assurer la pérennité des Documents technologiques :

- Mettre en place des alertes relatives aux formats d'encodage des Documents technologiques afin d'aviser la personne à l'origine du dépôt de l'obsolescence du format;
- Assurer la disponibilité et l'accessibilité des Documents technologiques conformément à l'*Entente de fourniture de service d'externalisation aux notaires* conclue avec la Chambre des notaires;
- Assurer la pérennité des technologies supportant les Documents technologiques pendant toute la durée de conservation prévue pour ces derniers.

Référence: ISO27001:2013 A-12

### 8.3 Gestion de la sécurité des réseaux

« Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient. »

Le Fournisseur doit utiliser un coupe-feu. Cependant, comme ce coupe-feu sécurise uniquement la communication nécessaire entre l'Internet et le serveur d'applications, et entre le serveur d'applications et le serveur de base de données, un système de prévention des intrusions doit servir de complément de protection logique au coupe-feu.

L'architecture doit être en mode trois tiers. De plus, la base de données et le serveur d'applications doivent être sur deux segments distincts.

La communication entre les consoles de gestion et les serveurs doit être chiffrée, à moins que la console soit directement connectée aux serveurs. Si elle est initiée de l'externe, la communication doit passer par un réseau privé virtuel (VPN).

Les réseaux de développement et de test ne doivent pas être dans le même sous-réseau IP (« *Internet Protocol* ») que les environnements de préproduction et de production.

Référence: ISO27001:2013 A-12

### 8.4 Manipulation des supports

« Empêcher la divulgation, la modification, le retrait ou la destruction non autorisée de biens et l'interruption des activités de l'organisme. »

Les médias, ou tout autre système ayant servi à offrir le Service d'externalisation ou ayant contenu les Documents technologiques, qui ne servent plus à fournir le Service d'externalisation doivent être détruits de façon sécuritaire. Par exemple, les médias doivent être détruits physiquement ou par écriture multiple avec confirmation d'exécution. Le but est de s'assurer que les Documents technologiques qui y étaient contenus ne sont plus récupérables, lisibles ou utilisables.

Référence: ISO27001:2013 A-12

## 8.5 Échange des informations

« *Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.* »

L'échange électronique d'information confidentielle doit être sécurisé, que ce soit entre le Fournisseur et une tierce partie, entre le Fournisseur et le notaire ou entre le Fournisseur et la Chambre des notaires. Dans le cas de médias contenant des Documents technologiques, le Fournisseur doit s'assurer d'utiliser un algorithme reconnu comme fiable pour le chiffrement des Documents technologiques et d'utiliser un transporteur offrant des garanties de sécurité et permettant une traçabilité des médias.

Si une synchronisation ou une sauvegarde des Documents technologiques est effectuée entre le serveur de base de données et un autre serveur, la communication doit être chiffrée si les Documents technologiques ne le sont pas.

Référence: ISO27001:2013 A-12.

## 8.6 Service de commerce électronique

« *Assurer la sécurité des services de commerce électronique, tout comme leur utilisation sécurisée.* »

Le Fournisseur doit assurer la protection contre les accès non autorisés. Ainsi, tout utilisateur doit être adéquatement authentifié (par exemple à l'aide d'un code utilisateur et mot de passe individuel) avant d'être autorisé à consulter ou modifier les Documents technologiques.

Référence: ISO27001:2013 A-12.

## 8.7 Surveillance

« *Détecter les traitements non autorisés de l'information.* »

La date et l'heure des serveurs et des équipements réseau doivent être synchronisées avec un serveur de temps.

Le Fournisseur doit conserver et protéger les journaux d'accès, d'événements de sécurité et d'activités sur les Documents technologiques pour une période d'au moins 12 mois. Les journaux doivent être analysés régulièrement afin de détecter toute anomalie sur les Actifs informationnels qui permettent d'offrir le Service d'externalisation.

Référence: ISO27001:2013 A-12, ISO27018:2014 12.4.2.

## 9. Contrôle d'accès du personnel du Fournisseur

### 9.1 Gestion de l'accès utilisateur

« *Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes d'information.* »

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:

- Un identifiant unique pour chaque utilisateur.
- Maintenir à jour une liste des utilisateurs.
- 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 :

- Vérification de l'identité de l'utilisateur avant de lui donner un nouveau mot de passe, que ce soit temporaire ou pour un remplacement.
- Les mots de passe temporaires doivent être transmis d'une manière sécuritaire.
- Les mots de passe doivent respecter les meilleures pratiques au niveau de la complexité, de la fréquence de changement et l'historique :
  - 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.
  - Éviter d'utiliser un mot de dictionnaire ou un mot qui ressemble au nom du Fournisseur, du service, du logiciel, du système ou de l'employé.
- Le verrouillage (temporaire ou permanent) des comptes doit être activé après un nombre défini de tentatives infructueuses.
- Un système doit engendrer une déconnexion automatique des sessions inactives après un délai défini.
- L'accès aux serveurs et aux équipements réseau doit être contrôlé au minimum par un identifiant et un mot de passe.
- Les identifiants génériques ne doivent être utilisés que lorsqu'il n'y a aucune alternative.
- 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.
- 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.
- 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.

## 9.2 Responsabilités utilisateurs

*« Empêcher les accès utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information. »*

Les utilisateurs, employés du Fournisseur, doivent:

- Utiliser les systèmes en respect des règles et politiques en vigueur.
- 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.

Référence: ISO27001:2013 A-9.

## 9.3 Contrôle d'accès au réseau

*« Empêcher les accès non autorisés aux services disponibles sur le réseau. »*

Les connexions à distance aux réseaux de production et de relève doivent être effectuées par Réseau Privé Virtuel (« VPN ») ou un canal sécurisé.

Aucun accès sans-fil non protégé ne doit être possible directement dans les environnements de production et de relève. Au minimum, le chiffrement WPA2 est requis.

Une authentification est requise pour se connecter sur les ports de diagnostics ou de configuration suivant les meilleures pratiques.

Référence : ISO27001:2013 A-9.

#### 9.4 Contrôle d'accès aux applications et à l'information

« Empêcher les accès non autorisés aux informations stockées dans les applications. »

Les infrastructures permettant d'offrir le Service d'externalisation doivent être logiquement isolées de tous les autres services pouvant être offerts par le Fournisseur.

Une authentification individuelle est requise pour accéder aux systèmes et aux Documents technologiques.

Référence: ISO27001:2013 A-9.

#### 9.5 Informatique mobile et télétravail

« Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail. »

Le chiffrement des Documents technologiques est requis sur tous les équipements mobiles. Ce chiffrement doit être effectué en utilisant un algorithme reconnu comme fiable.

Référence: ISO27001:2013 A-9.

### 10. Développement et maintenance des systèmes

#### 10.1 Bon fonctionnement des applications

« Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les 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.). Voir également la section 10.4.

Référence: ISO27001:2013

#### 10.2 Mesures cryptographiques

« Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques. »

Les Documents technologiques entreposés chez un Fournisseur doivent être chiffrés, à moins que d'autres mesures de protection équivalentes ou supérieures ne soient mises en place.

Les Documents technologiques doivent être chiffrés avant de quitter tout système informatique du Fournisseur ou du notaire. Si le document technologique lui-même n'est pas chiffré, un tunnel chiffré doit être utilisé entre les systèmes informatiques pour sécuriser les Documents technologiques en transit.

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 Documents technologiques accessibles au notaire, à la Chambre des notaires ou à une personne autorisée en vertu de la loi, notamment un syndic de la Chambre des notaires.

Référence: ISO27001:2013 A-10.

### 10.3 Sécurité des fichiers système

« Garantir la sécurité des fichiers système. »

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

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.

Référence: ISO27001:2013

### 10.4 Sécurité en matière de développement et d'assistance technique

Les Renseignements confidentiels ne doivent jamais être copiés dans les environnements de développement, de test et/ou de pré-production, à moins que ces environnements offrent des mesures de sécurité comparables à celles de l'environnement de production ou que les Documents technologiques aient été rendus anonymes.

Référence: ISO27001:2013 A-14.2

### 10.5 Gestion des vulnérabilités techniques

« Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication. »

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 correctifs de sécurité, tant applicatifs que systèmes, doivent être testés et appliqués dans un délai raisonnable afin d'assurer la sécurité générale des Actifs informationnels dans un délai raisonnable.

Référence: ISO27001:2013 A-14.2

## 11. Gestion des Incidents liés à la sécurité de l'information

### 11.1 Signalement des événements et des failles liés à la sécurité de l'information

« Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais. »

Le Fournisseur doit mettre en place des mesures de sécurité efficaces pour détecter les Incidents liés à la sécurité de l'information pouvant avoir un impact sur la confidentialité, l'intégrité ou la disponibilité des Documents technologiques ou du Service d'externalisation. Tout Incident lié à la sécurité de l'information détecté doit être inscrit dans un registre et rapporté aux notaires concernés et à la Chambre des notaires dans les 48 heures (plus spécifiquement au secrétaire de l'Ordre), notamment dans les cas suivants :

- Une perte ou un vol de Documents technologiques découlant du Service d'externalisation, que cette menace se produise du côté du client-notaire ou du Fournisseur (si celui-ci en est avisé).
- Une panne prolongée des systèmes servant à offrir le Service d'externalisation.
- Une compromission (ex. : piratage) des systèmes du Fournisseur.

À cet effet, le Fournisseur doit avoir une politique et un processus clairs pour la gestion des Incidents liés à la sécurité de l'information au sein de son organisation et pour la notification de ces derniers. Le Fournisseur doit conserver tous les Documents technologiques et les preuves

relatives aux Incidents liés à la sécurité de l'information pendant cinq (5) ans (incluant le nom des témoins, la période, les Documents technologiques et clients affectés). Il doit également assurer l'intégrité de ces preuves.

Référence: ISO27001:2013 A-16, ISO27002:2013, ISO27018:2014 s.16

## 12. Gestion du plan de continuité de l'activité

### 12.1 Aspects de la sécurité en matière de gestion de la continuité de l'activité

*« Neutraliser les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais. »*

Un processus de continuité des affaires du Fournisseur doit être implanté afin de minimiser les impacts d'une indisponibilité des Actifs informationnels ou du Service d'externalisation à un niveau acceptable par la Chambre des notaires. Ces indisponibilités pourraient être causées, par exemple, par une catastrophe naturelle, un accident, un Incident lié à la sécurité de l'information, un bris d'équipement ou un acte délibéré.

Le processus de continuité des affaires doit inclure les points suivants:

- Identification des rôles et responsabilités.
- Identification des procédures:
  - Procédure d'urgence;
  - Procédure de recouvrement;
  - Procédure de restauration;
  - Procédure opérationnelle temporaire;
  - Procédure de reprise des opérations normales.
- Identification du niveau acceptable pour l'indisponibilité du Service d'externalisation. À cet effet, le Fournisseur doit assurer la disponibilité des Actifs informationnels en moins de 4 heures lorsque survient une Interruption du Service d'externalisation. Dans les cas de Force majeure, le Fournisseur doit rendre les Actifs informationnels disponibles en moins de 72 heures.
- Documentation et mise en place des procédures de recouvrement et de restauration du Service d'externalisation ou des Documents technologiques.
- Inventaire des Actifs informationnels (serveurs, logiciels, licences, etc.)
- Tests documentés et mise à jour du plan de continuité des affaires au moins une fois par année.

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

Tout site de relève désigné pour le Service d'externalisation doit être situé en territoire canadien et:

- (i) à au moins vingt (20) kilomètres à vol d'oiseau du site de production; ou, alternativement
- (ii) à un endroit préalablement autorisé par écrit par la Chambre des notaires, dont la situation permet raisonnablement de croire qu'une même catastrophe (Force majeure ou non) n'affecterait pas concurremment le site de production et le site de relève désigné pour le Service d'externalisation.

Il appartient au Fournisseur de faire la démonstration que sont réunies les conditions nécessaires à (ii). La Chambre des notaires ne peut refuser son autorisation préalable que pour des motifs sérieux.

Référence: IS027001:2013 A-17

### **13. Remise des Actifs informationnels aux notaires**

Lorsque le Fournisseur doit effectuer une remise des Actifs informationnels qui lui ont été confiés, cette remise doit en comprendre la totalité et s'effectuer de façon sécurisée. Pour ce faire, le Fournisseur peut soit chiffrer les Documents technologiques ou utiliser un moyen de transfert sécurisé, tel que SFTP ou FTPS. Le Fournisseur doit ensuite détruire les Documents technologiques sur ses équipements conformément aux dispositions pertinentes de l'Entente de fourniture de service d'externalisation aux notaires.

### **14. Destruction sécuritaire des Documents technologiques**

Lorsque la destruction des Documents technologiques est requise, le Fournisseur doit les détruire de façon sécuritaire et permanente. Le Fournisseur doit produire au notaire ou à la Chambre une déclaration écrite à cet effet, sur simple demande du notaire ou de la Chambre selon le cas, et indiquer le procédé utilisé pour la destruction.

### **15. Signature numérique des notaires**

Si le Fournisseur utilise la signature numérique du notaire dans le cadre du Service d'externalisation, cette utilisation doit être conforme aux directives de Solutions Notarius Inc. et/ou Notarius - technologies et systèmes d'information notariale Inc. sur le sujet.