1. INFORMATIONS GÉNÉRALES

- **Technologie de signature** : Le concepteur doit décrire le type de technologie de signature offert aux clients finaux, qu'elle soit numérique ou électronique.
  - Détails : Décrire sommairement le processus de signature ainsi que les avantages de la technologie proposée.
- **Sécurité de la technologie :** Le concepteur doit aussi détailler les mécanismes de sécurité mis en place pour prévenir les menaces internes et externes à la sécurité informatique, tels que des politiques, procédures, outils de sécurité, etc.
  - Détails **:** Est-ce que le concepteur répond aux diverses exigences de sécurité nécessaires pour se conformer aux lois applicables, comme la *Loi sur la protection des renseignements personnels dans le secteur privé*, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), ainsi que les normes de sécurité telles que ISO 3200 et ISO 27001?
- **Hébergement** : L'OACIQ privilégie l'hébergement au Québec et au Canada puisque les normes en matière de protection des renseignements personnels y sont reconnues et sûres. À noter que la loi exige qu'une évaluation des facteurs relatifs à la vie privée (EFVP) soit réalisée par l'entreprise si les informations, y compris les renseignements personnels, sont communiquées et entreposées à l'extérieur du Québec.
- **Hébergement de la solution** : Le concepteur doit indiquer le ou les lieux d'hébergement de la solution, ainsi que les sites de relève.
- **Hébergement des formulaires signés** : Le concepteur doit indiquer le ou les lieux d'hébergement du stockage des données, ainsi que les sites de relève. Dans le cas d'un intégrateur de technologie de signature, il est important de mentionner le lieu d'incorporation du fournisseur de la technologie de signature.
- **Système de redondance** : Le concepteur doit indiquer la stratégie de redondance mise en place pour garantir une haute disponibilité.
  - Détails : Si aucune stratégie ou système de redondance n'est en place, le concepteur doit indiquer :
    - la période maximale pendant laquelle une perte d'information peut survenir en lien avec la stratégie de sauvegarde;
    - le processus prévu pour prévenir la perte d'information advenant un bris d'équipement entre deux sauvegardes.

2. GESTION DES FORMULAIRES OACIQ

- **Format des fichiers pour le chargement des formulaires à signer** : Le concepteur doit indiquer les formats de fichiers acceptés sur lesquels l'utilisateur pourra apposer sa signature.

- **Personnalisation des zones de signature** : Le concepteur doit indiquer quels types d'utilisateurs sont autorisés à personnaliser les diverses zones de signature et préciser le nombre maximal de signatures par formulaire.
- **Sauvegarde des zones de signature sous forme de gabarit** : Le concepteur doit indiquer si la solution permet de sauvegarder des gabarits de formulaires avec des zones de signature préétablies, et de créer une bibliothèque de formulaires à signer.
  - Détails : Ainsi, lorsque l'utilisateur voudra faire signer un formulaire existant, il ne lui sera pas nécessaire de définir les zones de signature, car elles auront été sauvegardées au préalable.
- **Stockage des formulaires prédéfinis sur le site du fournisseur** : Le concepteur doit indiquer s'il est possible de conserver une bibliothèque de formulaires prédéfinis, préciser la limite de formulaires pouvant être conservés ainsi que les formats de fichiers acceptés.
- **Jumelage automatique du formulaire chargé avec un gabarit prédéfini** : Le concepteur doit indiquer si le système permet de jumeler automatiquement un formulaire chargé par l'utilisateur avec un formulaire prédéfini contenu dans la bibliothèque de formulaires.
- **Interface multilingue — anglais et français** : Le concepteur doit fournir une copie des interfaces de gestion des formulaires afin d'en valider la qualité.
- **Personnalisation de l'interface** : Le concepteur doit indiquer si l'interface de gestion des formulaires peut être personnalisée aux couleurs et logos d'un courtier.
  - Détails : Un exemple de personnalisation doit être fourni.

3. GESTION DES SIGNATAIRES, SÉCURITÉ DES ACCÈS

- **Gestion de multiples signataires** : Le concepteur doit indiquer si le système permet la gestion de plusieurs signataires, tant pour l'acquéreur que pour le vendeur, et préciser le nombre maximal de signataires.
- **Gestion du flux/séquence des signataires** : Le concepteur doit décrire le processus de gestion des signataires.
  - Détails : Il doit expliquer comment l'utilisateur peut contrôler le flux de signatures des signataires selon l'une des deux options suivantes :
    - ✓ *Processus en série/séquence* : Sous-entend qu'un ensemble de formulaires à signer ne pourra être transmis au prochain signataire que lorsque le premier signataire aura terminé avec succès la signature de l'ensemble des formulaires ;
    - ✓ *Processus en parallèle* : Sous-entend qu'un ensemble de formulaires à signer peut-être transmis à tous les signataires simultanément et indépendamment de l'état d'achèvement.

- Dans le cas où les signataires sont représentés par différents intervenants, le système de signature électronique ou numérique doit permettre un processus d'affaires.

- **Personnalisation des courriels à l'ensemble des signataires** : Le concepteur doit fournir un exemple de courriel personnalisé envoyé aux signataires.
  - Détails : Si la personnalisation n'est pas permise, le concepteur doit fournir un exemple du message standard qui sera transmis aux signataires.
- **Personnalisation de la langue du courriel par le signataire** : Le concepteur doit indiquer si la langue du courriel qui sera envoyé à chaque signataire peut être personnalisée.
- **Niveaux de sécurité (vérification de l'identité du signataire) :** Le concepteur doit décrire le processus et les différentes méthodes qui permettront de s'assurer de l'identité numérique du signataire avant de pouvoir accéder au site contenant les formulaires à signer.
  - Détails : La validation de l'identité du signataire doit combiner au moins deux des méthodes suivantes :
    - ✓ Une **preuve d'identité** avec une validation à travers des documents officiels, comme la carte d'assurance maladie, le passeport, le permis de conduire, etc.
    - ✓ Une **confirmation basée sur les connaissances** qui peut être statique (utilisation de renseignements personnels recueillis antérieurement ou établis à un moment précis dans le temps) ou dynamique (utilisation de renseignements personnels recueillis ou générés au fil du temps).
    - ✓ Une **confirmation des caractéristiques biologiques ou comportementales** (comparaison des traits faciaux, de l'iris, des empreintes digitales, de la voix, analyse des données, etc.).
    - ✓ Une confirmation par un arbitre de confiance (répondant, notaire, agent agréé)
    - ✓ Une **confirmation par un élément connu de l'utilisateur** (par exemple, des jetons à secret mémorisé ou des jetons à renseignement préenregistré), par un **élément que l'utilisateur possède** (par exemple, un jeton à secret matriciel, un jeton hors bande, un dispositif de mot de passe à usage unique et à un seul facteur, ou un dispositif cryptographique à un seul facteur) ou par un **élément que l'utilisateur produit ou qui le caractérise** (comme les données biométriques telles que l'empreinte digitale, le balayage rétinien et la reconnaissance faciale).

      La confirmation peut comporter une interaction sécurisée avec un processus de validation physique ou électronique comme une notification *push* sur un dispositif hors bande comme un téléphone intelligent.

La méthode de vérification d'identité utilisant une pièce d'identité valide avec photo délivrée par un gouvernement devrait être privilégiée, car elle présente un risque plus faible par rapport aux autres méthodes.

- **Sécurité des transactions :** Le concepteur doit fournir des garanties sur la sécurité des signatures électroniques. Pour cela, il doit :

  ✓ **Garantir l'intégrité du document signé**
  Le concepteur doit démontrer qu'un document signé ne pourra être altéré. Il doit décrire le processus de certification des documents PDF utilisés afin d'en assurer l'authenticité.

  - Détails : Une fois le processus de signature terminé, les documents doivent être scellés électroniquement à l'aide d'un sceau numérique inviolable généré par une infrastructure à clé publique (ICP). Ce sceau confirme la validité de la signature et garantit que le document électronique n'a subi aucune altération ou modification depuis sa date de signature.
    Si le concepteur n'utilise pas de signature numérique, il doit démontrer que le processus utilisé garantit le caractère authentique des documents signés.

  ✓ **Délivrer un certificat d'achèvement**
  Ce certificat électronique renforce la sécurité de la signature digitale en fournissant des informations détaillées sur chaque signataire. Ces informations doivent inclure la déclaration du consommateur confirmant l'accord du signataire à utiliser la signature sous forme électronique, l'image de cette signature, les horodatages associés aux événements clés, l'adresse IP du signataire et d'autres données d'identification. Ces éléments contribuent à valider et authentifier la signature électronique du signataire.

- **Journalisation des transactions :** Le concepteur doit démontrer la procédure de suivi des transactions faites dans le système. Pour ce faire, il doit fournir, pour chaque transaction, une piste d'audit qui va agir comme un enregistrement électronique de toutes les actions effectuées sur le document numérique. Cette piste d'audit doit détailler l'historique et l'horodatage, qui lie la date et l'heure aux données de manière à exclure raisonnablement toute modification indétectable des données, et doit être basée sur une horloge précise liée au temps universel coordonné. Elle doit inclure les moments où le document a été ouvert, consulté et signé. En cas de contestation ou de doute sur une signature électronique, cette piste d'audit, accessible à tous les participants à la transaction, permet de fournir des preuves et de résoudre les objections.
  - Details: Le concepteur doit fournir une copie du journal des transactions.
- **Considérations pour une validation à long terme :** Le concepteur doit démontrer que tous les renseignements nécessaires à la validation de la signature électronique seront disponibles aussi longtemps que l'enregistrement sera conservé. La signature électronique doit pouvoir être vérifiée et confirmée au fil du temps.

- **Attribution des accès :** Le concepteur doit indiquer les outils de gestion des accès. Il doit indiquer quels groupes ou individus sont autorisés à accorder des accès, ainsi que les mécanismes garantissant la confidentialité d'accès des individus, tels que la modification des mots de passe.
  - Details: Étant donné que l'utilisateur peut utiliser le système de signature sans être membre d'une chambre immobilière, il est important de savoir si le concepteur exige que l'OACIQ soit l'unique responsable de l'attribution des accès. Si tel est le cas, cette solution ne serait ni souhaitable ni viable.
- **Groupe d'utilisateurs :** Le concepteur doit indiquer les groupes d'utilisateurs qui ont accès au système. Cette description doit définir les utilisateurs faisant partie de ces groupes, ainsi que leurs droits et privilèges — administrateur, utilisateur, signataire, etc. La gestion des accès doit respecter les principes du « moindre privilège » (un concept de sécurité selon lequel on accorde à un utilisateur le niveau d'accès [ou les permissions] minimum nécessaire pour accomplir son travail) et du « besoin de savoir » (principe selon lequel l'accès à un fichier doit être donné qu'à des utilisateurs dûment autorisés et authentifiés) pour minimiser le risque d'exposition des données.
- **Maintien de la confidentialité d'accès :** Le concepteur doit indiquer les mécanismes permettant d'assurer le maintien de la confidentialité d'accès des utilisateurs, particulièrement lorsque l'application est accessible aux clients et nécessite une authentification électronique. Des mécanismes tels que l'authentification multiple sont attendus.
- **Résiliation des droits d'accès :** Le concepteur doit décrire les processus permettant d'interrompre l'accès au système pour les utilisateurs qui n'ont plus les privilèges d'accès, quelle qu'en soit la raison (changement d'agence, fin de l'abonnement au service, etc.). Le processus doit permettre de détecter rapidement la résiliation de l'accès et d'interrompre immédiatement l'accès.

4. GESTION DU FLUX DES SIGNATAIRES

- **Saisie d'une date d'expiration — délai de signature pour le flux de signataires** : Le concepteur doit indiquer si le système permet de définir un délai de signature, que ce soit une date de fin ou un délai en heures ou en jours.
- **Gestion du délai des rappels aux signataires** : Le système doit permettre un mécanisme de suivi et de rappel pour informer les signataires qu'un document ou une série de documents sont prêts à être signés. Le concepteur doit fournir un exemple de ce rappel, disponible en français.
- **Alerte automatique au gestionnaire du processus — courriel** : Le système doit permettre d'aviser automatiquement par courriel l'utilisateur ou le gestionnaire afin de suivre l'état d'avancement du processus de signature. Tous les signataires doivent recevoir une confirmation une fois le processus complété, leur permettant de télécharger et sauvegarder le document.
- **Visualisation de l'état d'avancement du processus de signature** : Le système devra permettre de visualiser à l'écran l'état d'avancement du processus de signature.

5. PROCESSUS DE SIGNATURE DES FORMULAIRES

- **Interface multilingue — anglais et français** : Le concepteur doit s'assurer que toutes les interfaces qui seront affichées aux signataires soient en anglais et en français.
- **Accessibilité par un navigateur – IE, Safari, Firefox, Chrome** : Le concepteur devra fournir la liste complète des navigateurs autorisés ainsi que leurs versions respectives.
- **Application Android, iPhone, iPad** : Il s'agit de déterminer si la solution de signature est accessible via une application spécifique sur les téléphones intelligents et les tablettes numériques. Le concepteur devra fournir une liste des plateformes autorisées.
- **Affichage et acceptation du consentement avant le début du processus de signature** : Le concepteur doit permettre d'afficher et d'exiger que le signataire accepte le consentement avant de démarrer le processus de signature.
  - Détails : Le concepteur doit permettre de personnaliser le formulaire de consentement en anglais et en français.
- **Plateformes acceptées pour le processus de signature** : Le concepteur doit spécifier les plateformes disponibles qui pourront être utilisées par les signataires durant le processus de signature.
- **Options de signature** : Le concepteur doit décrire les diverses options de signature disponibles pour les signataires. L'utilisation du clavier avec sélection du type de calligraphie serait une option de base minimale.
- **Navigation assistée aux zones de signature** : Le concepteur doit permettre au signataire de naviguer rapidement entre les zones de signature, et l'informer du pourcentage ou du stade d'achèvement du processus de signature.
- **Zones de signature bien identifiées** : Le système doit clairement indiquer les zones précises où les signatures ou les initiales doivent être apposées par le signataire.
- **Sauvegarde du formulaire signé** : Le système doit permettre de sauvegarder le formulaire signé sur la plateforme du signataire, ainsi que d'héberger et de stocker les formulaires sur le ou les serveurs du concepteur ou du fournisseur de la solution.
- **Capacité d'exporter un ensemble de documents signés** : Le concepteur doit permettre au gestionnaire du processus de signature de sélectionner et d'exporter un ensemble de documents signés en format PDF.

6. INCLUSIONS OBLIGATOIRES OU ÉQUIVALENTES AU CONTRAT LIANT LE FOURNISSEUR ET LES CLIENTS

- Les clauses contractuelles énoncées ci-dessous, ou des clauses équivalentes, doivent obligatoirement être incluses dans tout contrat liant le fournisseur à un client, en anglais ou en français, selon la langue du contrat.
- Le fournisseur doit fournir, en vue de son accréditation par l'OACIQ, une copie du contrat qu'il prévoit utiliser dans ses relations d'affaires avec les clients.
- Si les clauses énoncées ci-dessous ne sont pas reproduites intégralement dans le contrat, des frais supplémentaires seront appliqués pour fin d'approbation des équivalences.

Préambule	**ATTENDU QUE** le Client est un courtier/une agence au sens de la *Loi sur le courtage immobilier* et ses règlements qu'il/elle est assujetti(e) au pouvoir de surveillance et de contrôle de l'Organisme d'autoréglementation du courtage immobilier du Québec (« OACIQ ») ainsi qu'aux pouvoirs du syndic de l'OACIQ;
Préambule	**ATTENDU QUE** le Client détient des données, des applications, des renseignements, des documents et informations confidentielles, incluant des renseignements personnels (ci-après l' « actif informationnel ») dont la cueillette, la conservation, l'utilisation, la communication et la destruction sont sujettes aux règlements adoptés en vertu de la *Loi sur le courtage immobilier* (c. C-73.2) et aux dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé* (c. P-39.1) (ci-après la « Loi sur le secteur privé »);
Préambule	**ATTENDU QUE**, conformément à ses obligations légales, le Client est tenu de protéger les renseignements personnels qu'il recueille, utilise, conserve, communique et détruit et qu'il est, entre autres, tenu d'aviser les personnes concernées du nom du tiers pour qui la collecte des renseignements personnels est faite, du nom du tiers à qui il est nécessaire de communiquer les renseignements personnels recueillis et de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec;
Préambule	**ATTENDU QUE**, conformément à ses obligations légales, le Client doit réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) en cas de communication et d'entreposage à l'extérieur du Québec des renseignements personnels qu'il détient;
Préambule	**ATTENDU QUE** le Client doit, s'il a des motifs raisonnables de croire qu'un *incident de confidentialité* au sens de la Loi sur le secteur privé s'est produit et que cet incident implique un renseignement personnel qu'il détient, prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent et qu'il doit aussi, si l'incident présente un risque sérieux de préjudice, en aviser les personnes concernées et les autorités compétentes;

Préambule	**ATTENDU QUE** le Client et le Fournisseur souhaitent, conformément aux obligations légales leur incombant, convenir des obligations et mesures destinées à assurer en tout temps le caractère confidentiel de l'actif informationnel du Client, y compris les renseignements personnels reçus, utilisés, conservés ou communiqués dans le cadre de l'exécution de ce contrat;
Protection de l'actif informationnel	**Le Fournisseur reconnait** qu'il est responsable en tout temps d'assurer la protection et le caractère confidentiel de l'actif informationnel, y compris les renseignements personnels, qu'il reçoit dans le cadre du présent contrat, que ce soit lors de leur communication, utilisation, détention, conservation et destruction.
Sous-traitants	**Le Fournisseur doit** encadrer les activités de ses sous-traitants et obtenir des engagements contractuels de leur part afin de s'assurer qu'ils respectent les obligations stipulées dans ce contrat, notamment celles relatives à la communication, l'utilisation, la conservation, la destruction et la protection des renseignements personnels. Le Fournisseur est garant envers le Client de la pleine exécution de ces obligations. Nonobstant les termes des ententes susceptibles d'intervenir entre le Fournisseur et ses sous-traitants, le Fournisseur est responsable de l'entièreté des obligations souscrites dans le présent contrat en regard des services, ainsi que du maintien de la confidentialité de l'actif informationnel. Il est garant envers le Client de la pleine exécution de ces obligations.
Cloisonnement de l'actif informationnel	**Le Fournisseur s'engage** à fournir les services et à conserver l'actif informationnel du Client de façon à en assurer le cloisonnement logique. Les parties reconnaissent que cela n'exclut pas le recours aux installations d'hébergement d'un tiers agissant comme sous-traitant du Fournisseur.
Équipements dédiés	*Note : Dans la mesure où la sensibilité de l'information le nécessite et justifie des coûts plus élevés, certains fournisseurs offrent des équipements dédiés. Le cas échéant, la clause suivante peut être utilisée :* **Le Fournisseur s'engage** à recourir à des équipements dédiés à la prestation des services afin d'assurer le cloisonnement de l'actif informationnel du client. Les parties reconnaissent que cela n'exclut pas le recours aux installations d'hébergement d'un tiers agissant comme sous-traitant du Fournisseur.
Restriction à localisation géographique	**Le Fournisseur s'engage** à aviser le Client de l'emplacement géographique des installations, équipements et systèmes utilisés dans le cadre de l'exécution du contrat et sur lesquels sera hébergé l'actif informationnel du Client. Le Fournisseur s'engage à n'utiliser que des installations ou équipements situés à l'intérieur des limites territoriales du Canada, de préférence au Québec. Le Fournisseur s'engage à aviser le Client sans délai et chaque fois que lui-même ou un sous-traitant, dans le cadre du présent contrat, a recours aux installations d'hébergement se situant à l'extérieur du Québec.

Avis et coopération en cas de demande ou ordonnance d'accès par des autorités	**Lorsque le Fournisseur ou l'un de ses sous-traitants reçoit une ordonnance émise par un tribunal**, une assignation (subpoena), ou toute autre requête d'une autorité compétente exigeant la communication de l'actif informationnel, le **Fournisseur s'engage** à en aviser immédiatement le Client, et ce, dans un délai maximal de quatre (4) heures. Les obligations du Fournisseur en vertu de ce paragraphe s'appliquent à toute demande entraînant l'accès ou la communication de l'actif informationnel du Client, indépendamment du fait que l'ordonnance, l'assignation, ou toute autre requête d'une autorité compétente porte spécifiquement ou non sur ceux-ci. Le Fournisseur s'engage, dans la mesure permise par les lois du Québec, à vérifier la légalité de la procédure d'émission ou d'obtention de l'ordonnance, de l'assignation ou de toute autre requête d'une autorité compétente. À moins qu'il ne s'agisse d'une requête de tout type provenant de l'OACIQ, le **Fournisseur s'engage** à s'opposer à l'ordonnance, à l'assignation ou à toute autre requête d'une autorité compétente, ou à demander un report de son exécution, afin de permettre au Client de réviser l'objet de ces demandes et, le cas échéant, de faire valoir ses droits ou ceux de ses clients. **Si le Fournisseur ne peut pas aviser le Client** en temps opportun, ou s'il est légalement empêché de le faire concernant une ordonnance, une assignation ou toute autre demande d'une autorité compétente, il s'engage à en informer le Client dès qu'il sera légalement autorisé à le faire. Le Fournisseur tiendra un registre des demandes, dans la mesure permise par les lois du Québec.
Confidentialité sécurité	**Le Fournisseur s'engage** à prendre et à appliquer des mesures de sécurité adéquates pour assurer la protection et la confidentialité, l'intégrité et l'accessibilité de l'actif informationnel du Client. Cela inclut le chiffrement des documents et des données au moment de leur transmission et pendant leur conservation, ainsi que dans les centres où l'actif informationnel est entreposé et conservé. Le Fournisseur s'engage aussi à prendre et à appliquer des mesures de contrôle d'accès, d'authentification des utilisateurs et de continuité des opérations, qui sont raisonnables compte tenu, notamment, de la sensibilité de l'actif informationnel reçu et/ou communiqué dans le cadre du présent contrat, de la finalité de son utilisation, de sa quantité et de son support. Les processus en place doivent également viser à empêcher les *incidents de confidentialité* au sens de la Loi sur le secteur privé, les atteintes à la sécurité, les erreurs (comme les modifications non encadrées des systèmes), la malveillance, ainsi que la divulgation ou la destruction non autorisée de l'actif informationnel. Le Fournisseur s'engage à se doter d'un mécanisme d'identification et de gestion des risques auxquels il est confronté, ainsi que d'un système d'audit ou de vérification permettant d'attester du respect des règles et processus en place.

Confidentialité sécurité	**Le Fournisseur reconnaît** qu'il se verra communiqué, et aura accès à l'actif informationnel confidentiel recueilli et conservé par le Client dans le cadre de ses activités. **Le Fournisseur reconnaît** que l'actif informationnel demeure la propriété exclusive du Client ou que celui-ci en est le détenteur au sens de la Loi sur le secteur privé; qu'il peut revendiquer cet actif informationnel, et que toute divulgation non autorisée, dont notamment des renseignements personnels, lui causerait des préjudices importants.
Confidentialité sécurité	**Le Fournisseur s'engage** à préserver le caractère confidentiel de l'actif informationnel tout au long de l'exécution du présent contrat et à prendre toutes les mesures appropriées à chacune des étapes de son exécution, à cette fin : • Préserver la confidentialité des codes d'utilisateur, mots de passe et clés de chiffrement selon les meilleures pratiques de l'industrie. • Exiger que toute personne désignée par le Fournisseur pour manipuler ou traiter l'actif informationnel signe au préalable un engagement de confidentialité et de respect des mesures de sécurité. Restreindre l'accès, la communication ou la divulgation de l'actif informationnel à ces seules personnes et effectuer une vérification des antécédents avant leur recrutement. • Utiliser l'actif informationnel, y compris les renseignements personnels, uniquement aux fins pour lesquelles il a été communiqué. • Ne pas communiquer l'actif informationnel du Client, y compris les renseignements personnels reçus ou communiqués dans le cadre du présent contrat à des tiers, sauf si cela est nécessaire pour l'exécution du présent contrat. Collaborer avec le Client, et ses clients le cas échéant, afin de permettre aux personnes visées d'exercer leur droit d'accès et de rectification de leurs renseignements personnels. • Collaborer avec le Client afin de détruire les renseignements personnels et les profils d'utilisateur en conformité avec le calendrier de conservation applicable. • Ne pas reproduire l'actif informationnel du Client, y compris les renseignements personnels reçus ou communiqués dans le cadre du présent contrat, sauf si une telle reproduction est nécessaire pour l'exécution du présent contrat. • Collaborer à toute enquête ou vérification concernant le respect de la confidentialité de l'actif informationnel, y compris les renseignements personnels.

Droit de vérification	**Le Fournisseur reconnaît** au Client le droit de vérifier à tout moment le respect des obligations mentionnées ci-dessus, ainsi que la conformité à la Loi sur le secteur privé et à la Loi sur le courtage immobilier incluant, si nécessaire, l'accès à ses installations. Le Fournisseur s'engage, au même titre que le Client, à collaborer à toute enquête ou vérification menée par les autorités compétentes, incluant l'OACIQ.
Avis et coopération en cas de violation de la confidentialité des renseignements personnels et/ou d'atteinte à la sécurité	**Le Fournisseur s'engage** à aviser le Client sans délai, et dans un délai maximal de quatre (4) heures, de toute violation ou tentative de violation des obligations de confidentialité des renseignements personnels communiqués dans le cadre du présent contrat. Cela inclut tout incident de confidentialité au sens de la Loi sur le secteur privé, tout accès ou tentative d'accès non autorisé, ainsi que toute atteinte au caractère confidentiel de l'actif informationnel du Client. **Le Fournisseur s'engage** au surplus à poser sans délai les actes nécessaires afin de pallier le risque d'atteinte continue, à procéder à une enquête afin d'identifier toute vulnérabilité et à apporter les correctifs nécessaires afin d'éviter toute répétition d'un tel incident. Le Fournisseur s'engage à permettre au Client ou à toute personne désignée par celui-ci d'effectuer toute vérification relative à la confidentialité des renseignements personnels. À cette fin, le Fournisseur autorisera le Client ou toute personne désignée par celui-ci à accéder à tout lieu, matériel, document ou équipement en lien avec toute violation ou tentative de violation de confidentialité des renseignements personnels. Les parties procéderont conjointement à l'analyse et à la gestion de la situation afin de minimiser les risques et d'identifier les intervenants appropriés en fonction du risque. Le Fournisseur s'engage à prendre toute mesure demandée par le Client pour diminuer le risque qu'un préjudice soit causé.
Assurance	**Le Fournisseur doit souscrire et maintenir** en vigueur pendant la durée du contrat à ses frais et auprès de compagnies d'assurance reconnues, une police d'assurance responsabilité professionnelle d'un minimum de cinq cent mille dollars (500 000 $ en dollars canadiens) par événement, avec une franchise n'excédant pas 10 000 $. Cette assurance doit couvrir, sans s'y limiter, les pertes et dommages résultant d'erreurs ou d'omissions dans l'exécution du contrat. De plus, cette police d'assurance professionnelle doit également inclure la même couverture pour les attaques de pirates informatiques (hackers) qui pourraient accéder illégalement à l'actif informationnel du Client, ainsi que pour toute erreur ou omission attribuable au Client. Elle doit également comporter un avenant contre la destruction, la modification, la perte ou autres incidents similaires concernant les données et informations, incluant les renseignements personnels et les documents du Client.
Terminaison, résiliation, annulation	**Le Fournisseur doit**, dans un délai de 30 jours suivant la date de la terminaison, la résiliation ou l'annulation du contrat, remettre au Client l'ensemble de l'actif informationnel reçu et/ou communiqué dans le cadre du

	présent contrat, et ce, quel que soit la nature des renseignements, documents ou informations ou le support sur lequel ils sont contenus. À compter de la date de la terminaison, de la résiliation ou de l'annulation du contrat, le Fournisseur s'engage à ne conserver aucune copie et à cesser toute utilisation de l'actif informationnel, y compris les renseignements personnels reçus et/ou communiqués dans le cadre du présent contrat. À la demande écrite expresse du Client, le Fournisseur s'engage à lui fournir une preuve à cet effet, jugée acceptable par le Client. Les obligations du Fournisseur relatives à la confidentialité des renseignements personnels reçus et/ou communiqués dans le cadre du présent contrat survivent à sa terminaison, à sa résiliation ou à son annulation.