ANNEXE CONCERNANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Cette Annexe concerne la protection des Renseignements personnels (ci-après l'« **Annexe de PRP** ») transmis ou mis à la disposition du Fournisseur ou autrement traités par le Fournisseur dans le cadre de **l'Annexe de PRP** qui inclut, entre autres, l'Annexe de Sécurité des Informations du Client (ci-après l'« **Annexe de Sécurité** ») qui lui est rattachée. La présente Annexe de PRP fait partie intégrante de l'Entente. La présente Annexe de PRP lie **la SADC d'Antoine-Labelle** (ci-après le « **Fournisseur** ») et **[ ]** (ci-après le « **Client** »). La présente Annexe de PRP fait partie intégrante de l'Entente. En cas de conflit entre les dispositions de l'Entente (ou de tout autre contrat) et ceux de la présente Annexe de PRP, les dispositions de la présente Annexe de PRP auront préséance.

La présente Annexe de PRP a, entre autres, pour objet d'assurer la conformité de l'Entente avec la *Loi sur la protection des renseignements personnels dans le secteur privé* ainsi que tout autre législations canadiennes, québécoises ou étrangères applicables en matière de protection des renseignements personnels qui pourraient s'appliquer au Québec ou à l'extérieur du Québec (collectivement les « **Lois sur la protection des renseignements personnels** »).

1. PRINCIPES

1.1. Le Fournisseur reconnaît que certains renseignements communiqués dans le cadre de cette Entente pourraient comprendre des renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier étant considérés comme des « **Renseignements personnels** » conformément aux Lois sur la protection des renseignements personnels. Tous Renseignements personnels sont de nature confidentielle.

1.2. Le Fournisseur s'engage à accéder, donner l'accès, publier, rectifier, altérer, collecter, utiliser, conserver, transférer, communiquer, anonymiser, dépersonnaliser, détruire et divulguer (ci-après « **Traiter** ») les Renseignements personnels (i) en stricte conformité avec l'Entente et ses Annexes et (ii) en stricte conformité avec les Lois sur la protection des renseignements personnels.

2. RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

2.1. Le Fournisseur doit nommer son Responsable de la protection des renseignements personnels selon les modalités prévues par les Lois sur la protection des renseignements personnels. Ce Responsable de la protection des renseignements veille à ce que les Renseignements personnels soient Traités et protégés conformément aux Lois sur la protection des renseignements personnels, à l'Entente et à ses Annexes. Le Responsable de la protection des renseignements personnels du Fournisseur doit disposer des connaissances, des compétences, des ressources et de l'autorité suffisantes pour remplir adéquatement ses fonctions.

2.2. Au plus tard cinq (5) jours après la signature de la présente Entente, le Fournisseur doit communiquer au Client les coordonnées de son Responsable de la protection des renseignements personnels désigné, incluant son nom et son prénom, son titre, son numéro de téléphone et son adresse courriel.

2.3. Tout remplacement du Responsable de la protection des renseignements personnels doit être communiqué par écrit, sans délai, au Client.

3. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

3.1. Le Fournisseur doit réaliser une Évaluation des facteurs relatifs à la vie privée (ci-après « EFVP ») lorsque celle-ci est imposée par la Loi.

3.2. Le Fournisseur doit communiquer sur demande au Client toutes documentations relatives aux EFVP qui concernent les opérations du Fournisseur, de ses mandataires ou de ses sous-traitants. Le Fournisseur doit prévoir dans ses contrats avec ses mandataires et sous-traitants la possibilité de communiquer, en toutes circonstances, leurs propres EFVP au Client.

3.3. Le Fournisseur doit assister le Client dans la réalisation de ses propres EFVP.

4. ACCÈS AUX RENSEIGNEMENTS PERSONNELS

4.1. Sans s'y limiter, le Fournisseur doit limiter l'accès aux Renseignements personnels selon les modalités prévues aux articles 8 et 9 de l'Annexe de sécurité.

4.2. Le Fournisseur doit Traiter les Renseignements personnels de manière strictement confidentielle et s'assurer que les employés, sous-traitants ou mandataires :

(a) ne puissent accéder qu'aux Renseignements personnels nécessaires pour l'exécution des obligations prévues par l'Entente;

(b) limitent l'accès aux Renseignements personnels selon les modalités prévues aux articles 8 et 9 de l'Annexe de sécurité ;

(c) soient informés du caractère confidentiel des Renseignements personnels;

(d) connaissent les dispositions des Annexes de l'Entente ;

(e) signent un engagement de confidentialité contenant des clauses de confidentialité et sur la protection des renseignements personnels similaires à celles énoncées dans la présente Annexe de PRP et l'Annexe de Sécurité;

(f) reçoivent des formations appropriées pour assurer le respect des Annexes de l'Entente et des Lois sur la protection des renseignements personnels; et

(g) se conforment à toutes exigences prévues par les Annexes de l'Entente et par les Lois sur la protection des renseignements personnels. Des sanctions appropriées doivent être implémentées en cas d'actions ou d'inactions non conformes à ces exigences.

5. TRAITEMENT DES RENSEIGNEMENTS PERSONNELS

5.1. Le Fournisseur devra assister le Client à respecter ses propres obligations légales, incluant celles concernant, sans s'y limiter :

(a) la sécurité des Renseignements personnels ;

(b) tout Traitement des Renseignements personnels;

(c) toute notification d'un Incident de sécurité requise par la Loi ; et

(d) toutes requêtes en provenance d'une personne concernée par un Renseignements personnels ou une institution publique.

5.2. Sauf instruction contraire écrite du Client, le Fournisseur ne peut Traiter des Renseignements personnels que si ce Traitement est nécessaire à l'exécution des obligations prévues par l'Entente ou par ses Annexes. Ce Traitement doit être conforme aux Lois sur la protection des renseignements personnels, aux obligations prévues par l'Entente et ses Annexes ainsi qu'aux instructions écrites du Client. Les employés, sous-traitants ou mandataires, ne peuvent accéder ou traiter les Renseignements personnels que lorsque cela est nécessaire à l'exercice des obligations prévues par l'Entente et ses Annexes.

5.3. Le Fournisseur s'engage à permettre au Client de Traiter ou d'altérer les usages et les fins des Renseignements personnels immédiatement après que le Client en formule la demande. Alternativement, le Fournisseur peut fournir l'accès des Renseignements personnels au Client (ou à un fournisseur de service du Client) et lui offrir les autorisations requises afin qu'il puisse lui-même Traiter ou altérer les usages et les fins des Renseignements personnels.

5.4. Sans limiter les obligations prévues à l'article 6 de l'Annexe de sécurité, le Fournisseur s'engage à (re)communiquer ou (re)transmettre au Client tous Renseignements personnels conservés par le Fournisseur et par ses mandataires, sous-traitants et agents (ci-après « **Agents** ») au moment de la résiliation ou de l'expiration de l'Entente. Immédiatement après avoir (re)communiquer ou (re)transférer les Renseignements personnels en question, le Fournisseur doit s'assurer de détruire complètement et de façon sécuritaire tous les Renseignements personnels conservés par le Fournisseur et par ses Agents.

6. DEMANDES DES PERSONNES CONCERNÉES

6.1. Le Fournisseur doit coopérer pleinement avec le Client et garantir la mise en place de mesures techniques et organisationnelles appropriées, en particulier pour :

(a) permettre au Client de s'acquitter de ses obligations légales de donner suite aux demandes des organismes publics et des personnes concernées par les Renseignements personnels dans l'exercice de leurs droits prévus aux Lois sur la protection des renseignements personnels, et ce, dans les délais prescrits par la Loi ;

(b) informer immédiatement le Client de toute demande, plainte ou allégation, relative aux Renseignements personnels, formulée par une personne concernée ou un organisme public ;

(c) tenir le Client au courant de toutes communications se rapportant à toute demande, plainte ou allégation relative aux Renseignements personnels ;

(d) à suivre les instructions du Client relativement à la demande, plainte ou allégation ; et

(e) à fournir immédiatement, à la demande du Client, tous Renseignements personnels dans le support choisi par le Client.

7. MESURES DE SÉCURITÉ

7.1. Le Fournisseur prend les mesures techniques, physiques et organisationnelles propres à assurer la confidentialité et la protection des Renseignements personnels. Le Fournisseur doit implémenter les mesures prévues dans l'Annexe de Sécurité afin d'assurer la protection des Renseignements personnels.

8. INCIDENTS DE CONFIDENTIALITÉ

8.1. Pour les fins de la présente Annexe de PRP et de l'Annexe de sécurité, un « **Incident de confidentialité** » est défini comme :

(a) l'accès non autorisé par la loi ou par la présente Entente à un Renseignement personnel ;

(b) l'utilisation non autorisée par la loi ou par la présente Entente d'un Renseignement personnel ;

(c) la communication non autorisée par la loi ou par la présente Entente d'un Renseignement personnel ; ou

(d) la perte d'un Renseignement personnel ou toute autre atteinte à la protection d'un tel Renseignement.

8.2. Lorsqu'un Incident de confidentialité est soupçonné ou confirmé, le Fournisseur doit Traiter l'incident au regard des obligations prévues à l'article 12 de l'Annexe de sécurité.

8.3. Le Fournisseur doit tenir un registre des Incidents de confidentialité. Ce registre doit minimalement contenir :

(a) une description des renseignements visés par l'incident ;

(b) les causes et circonstances de l'incident ;

(c) la date réelle ou présumée de l'incident ;

(d) la date de la connaissance de l'incident ;

(e) le nombre de personnes concernées par les Renseignements personnels touchés par l'incident ;

(f) une estimation de la gravité du risque de préjudice et les raisons qui motivent cette conclusion ;

(g) lorsqu'applicable, la date de transmission des avis aux personnes concernées ou à la Commission d'accès à l'information ; et

(h) les mesures que le Fournisseur a et prévoit implémenter afin de réduire la probabilité que l'incident ne se reproduise pas et afin de limiter les préjudices pouvant résulter de l'incident.

8.4. Si le Client en fait la demande, le Fournisseur doit lui communiquer son Registre des incidents de confidentialité Client dans les cinq (5) jours suivant sa demande.

9. TRANSFERT ET COMMUNICATION HORS QUÉBEC

9.1. Le Fournisseur doit conserver tous les Renseignements personnels communiqués par le Client au Québec.

9.2. À moins d'obtenir le consentement préalable du Client, le Fournisseur ne peut ni transférer ni communiquer des Renseignements personnels à l'extérieur du Québec. Il ne peut pas non plus confier à une entité à l'extérieur du Québec la tâche de Traiter des Renseignements personnels. Le consentement du Client doit être écrit, manifeste, et spécifique. Le Fournisseur ne peut communiquer ou transférer les Renseignements personnels que s'il respecte les conditions et modalités prévues par l'autorisation, l'Annexe de Sécurité et par les Lois sur la protection des Renseignements personnels.

9.3. À moins d'instruction contraire du Client, le Fournisseur doit cesser immédiatement toute communication ou transfert de Renseignements personnels à l'extérieur du Québec dès qu'il prend connaissance d'une possible violation des conditions et modalités prévues à l'article 9.2. En pareilles circonstances ou en cas de résiliation ou d'expiration de l'Entente, il doit également exiger le retour et la destruction des Renseignements personnels.

10. RESPONSABILITÉ ET INDEMNISATION

10.1. Le Fournisseur sera tenu, à la demande du Client, d'intervenir dans sa défense et d'indemniser le Client des dépenses, pertes, coûts dommages subis par le Client si ce dernier est mis en cause ou devient partie à toute procédure ou enquête de nature judiciaire ou administrative engagée par un tiers ou par un organisme public en raison :

(a) d'une violation par le Fournisseur ou l'un de ses mandataires ou sous-traitants d'une obligation prévue par l'Entente ou de l'une de ses Annexes ;

(b) d'un Incident de confidentialité concernant un ou plusieurs Renseignements personnels Traités; ou

(c) de tout manquement à une loi ou un règlement qui protègent les Renseignements personnels.

Ces dépenses, pertes, coûts et dommages incluent, sans s'y limiter, tout montant et intérêt, auquel le Client ou le Fournisseur pourraient se voir contraints de verser en conséquence d'une pénalité, sanction, ordonnance, jugement ou règlement, ainsi que de tous les frais judiciaires et extrajudiciaires encourus par le Client en raison de la mise en cause ou de la plainte, procédure judiciaire, procédure administrative ou enquête.

11. AMENDEMENT

11.1. Le Client peut décider, à son entière discrétion, de modifier la présente Annexe de PRP afin, entre autres, d'y introduire, d'y modifier ou d'y éliminer des obligations, des pratiques, des mesures ou des procédures afin d'assurer la conformité du Fournisseur, la conformité d'un Sous-traitant ou la conformité du Client aux exigences légales ou réglementaires.

12. SURVIE

12.1. Nonobstant les dispositions de résiliation prévues à l'Entente ou à tout contrat entre les Parties, dans la mesure où le Fournisseur continue d'avoir accès à des Renseignements personnels pour quelque raison que ce soit, le Fournisseur continuera à être lié par les termes de la présente Annexe de PRP. Il reste en tout temps lié à ses obligations prévues à l'article 10 de la présente Annexe de PRP.

SIGNÉ À _____, ce _____

SADC d'Antoine-Labelle	**[ ]**
(FOURNISSEUR)	**(CLIENT)**
Par : _____	Par : _____
Nom du Représentant	Nom du Représentant
_____	_____
Titre du Représentant	Titre du Représentant
_____	_____
Signature du Représentant	Signature du Représentant

ANNEXE DE SÉCURITÉ DES INFORMATIONS DU CLIENT

La présente annexe concerne la sécurité de l'information (ci-après l'« **Annexe de sécurité**»). Elle énonce les obligations entre **[ ]** faisant affaire sous le nom **[ ]** (ci-après le « **Client** ») et **la SADC d'Antoine-Labelle** (ci-après le « **Fournisseur** ») concernant la sécurité de l'information dans le cadre de la **Loi 25 sur la protection des renseignements personnels** (ci-après l'« **Entente** »), incluant notamment l'Annexe concernant la protection des renseignements personnels (ci-après l' « **Annexe de PRP** ». En cas de conflit entre les dispositions de l'Entente (ou de tout autre contrat) avec le Fournisseur et ceux de la présente Annexe de sécurité, les dispositions de la présente Annexe de sécurité auront préséance.

1. EXIGENCES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

1.1. Le Fournisseur doit mettre en place des mesures de sécurité et des processus opérationnels adéquats pour assurer la protection de l'information du Client qui est transmise ou autrement communiquée dans le cadre de l'Entente (ci-après « **Information du Client** »). L'appellation « Information du Client » comprend, sans s'y limiter, tous les renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier étant considérés comme des « **Renseignements personnels** » conformément aux Lois sur la protection des renseignements personnels.

1.2. Le Fournisseur doit préserver la confidentialité, l'intégrité et la disponibilité de l'Information du Client. Il doit également empêcher l'accès, la collecte, la divulgation, la publication, le transfert, la communication, l'utilisation, la diffusion, la destruction, la rectification, la modification, la conservation, l'anonymisation, la dépersonnalisation ou l'altération (ci-après le « **Traitement** ») non autorisés de l'Information du Client.

1.3. L'Information du Client doit être protégée selon les normes et standards reconnus de l'industrie en matière de sécurité de l'information. Cette protection doit être conforme aux obligations imposées par les Lois sur la protection des renseignements personnels, par l'Entente et par ses Annexes.

2. GOUVERNANCE

2.1. Le Client se réserve le droit de convoquer sans préavis des rencontres de gouvernance afin d'assurer la conformité de sécurité de l'Information. Le Responsable de la protection des renseignements personnels du Fournisseur doit être présent à cette rencontre.

2.2. Le Fournisseur est tenu de répondre par écrit aux questions soulevées lors de la rencontre de gouvernance, au plus tard dix (10) jours ouvrables après leur réception.

2.3. Un plan formel de gouvernance des risques incluant des politiques, procédures et contrôles internes doivent exister. Les risques inhérents au Traitement de l'Information du Client doivent être identifiés, classifiés et mitigés selon une norme reconnue de l'industrie. Les personnes et actifs impliqués dans cette gestion de risques doivent être préalablement identifiés, de même que tous les risques inhérents, et être approuvés par le Client.

3. POLITIQUE DE SÉCURITÉ

3.1. Le Fournisseur doit maintenir des pratiques en matière de sécurité qui permettent de réduire les risques liés aux ressources humaines. Ces pratiques doivent être consolidées dans une politique approuvée par le Fournisseur. Le Fournisseur doit assurer la révision et la maintenance de ladite politique (ci-après « **Politique de sécurité** »).

3.2. La Politique de sécurité du Fournisseur doit être documentée, révisée régulièrement et communiquée aux personnes appropriées dans son entreprise. Cette politique doit minimalement :

(a) couvrir les différentes opérations et mesures de sécurité imposées par le Fournisseur, ses consultants, ses mandataires et ses sous-traitants (ci-après « **Agents** ») aux Informations du Client à chacune des étapes de leur cycle de vie ;

(b) prévoir l'encadrement applicable au Traitement de l'Information du Client selon les modalités prévues à l'Entente et à ses Annexes ;

(c) prévoir les rôles et les responsabilités des membres du personnel et des Agents du Fournisseur tout au long du cycle de vie de l'Information du Client ;

(d) prévoir une gestion des accès et des permissions des membres du personnel à l'Information du Client selon les modalités prévues aux articles 8 et 9 de la présente Annexe de sécurité;

(e) prévoir un processus de traitement des plaintes relatives à la protection des Renseignements personnels ; et

(f) prévoir toutes autres mentions requises par les Lois sur la protection des renseignements personnels.

3.3. Le Fournisseur et ses Agents doivent s'assurer qu'aucun employé détenant des antécédents judiciaires n'est autorisé à accéder aux Informations du Client dans la mesure où de tels antécédents seraient incompatibles avec la sécurité des Informations du Client. Le Fournisseur, ses sous-traitants et mandataires, doivent effectuer la vérification des antécédents judiciaires auprès d'une firme reconnue tous les 3 ans pour ses employés ayant des accès aux Informations du Client ou accès aux supports, équipements et systèmes qui Traitent ces Informations.

3.4. Le Client peut effectuer la vérification des antécédents judiciaires pour les employés du Fournisseur et de ses Agents si ces employés peuvent accéder aux Informations, aux systèmes ou aux sites du Client. Le Fournisseur doit communiquer toutes les informations nécessaires à cette vérification et, si nécessaire, obtenir tout consentement nécessaire à leur communication et utilisation.

3.5. Le Fournisseur doit être en mesure de fournir dans des délais raisonnables, sur demande du Client, les Politiques de sécurité de ses Agents ainsi que sa propre Politique de sécurité. Le Fournisseur doit également fournir dans des délais raisonnables, sur demande du Client, la liste des personnes impliquées dans l'exécution de l'Entente. Cette liste doit identifier, sans se limiter à, toutes les personnes ayant accès aux supports, équipements et systèmes qui Traitent cette information.

4. FORMATION ET SENSIBILISATION AUX ENJEUX DE SÉCURITÉ

4.1. Le Fournisseur doit sensibiliser régulièrement tous ses Agents aux enjeux de sécurité de l'information. En outre, le Fournisseur doit mettre en place un code de conduite et une politique d'usage acceptable des technologies de l'information. Ces documents devront être lus et acceptés par toutes personnes impliquées dans l'exécution de l'Entente.

4.2. Le Fournisseur doit organiser une formation annuelle en vue de sensibiliser ses employés et Agents à la sécurité de l'information et des renseignements personnels, aux nouveaux enjeux en matière de sécurité de l'information, aux obligations prévues par les Annexes de l'Entente ainsi qu'aux Lois sur la protection des renseignements personnels.

5. GESTION DES ACTIFS INFORMATIONNELS ET PHYSIQUES

5.1. Le Fournisseur doit assurer une gestion adéquate des actifs informationnels utilisés pour l'exécution des obligations prévues par l'Entente. Le Fournisseur doit identifier et répertorier ses

actifs physiques et logiques contenant de l'Information du Client, incluant les équipements informatiques et supports-papier. Tous les actifs doivent être classifiés et catégorisés en fonction de l'information contenue selon une procédure formelle.

6. DESTRUCTION DE L'INFORMATION DU CLIENT

6.1. À moins d'instructions contraires du Client, le Fournisseur s'engage à, lorsque la Loi le permet, le (re)communiquer ou (re)transmettre au Client toutes Informations du Client conservées par le Fournisseur et par ses Agents dans les circonstances suivantes :

(a) dans un délai raisonnable suivant une demande écrite du Client ;

(b) au moment de l'exécution d'un plan de transition ; et

(c) dès l'expiration ou de la résiliation de l'Entente.

Immédiatement après avoir (re)communiquer ou (re)transférer les Informations du Client, le Fournisseur doit s'assurer de détruire complètement et de façon sécuritaire toutes les Informations du Client conservées par le Fournisseur et par ses Agents.

6.2. Les méthodes de destructions utilisées par le Fournisseur pour procéder à la destruction de l'Information doivent respecter la Loi, les normes et réglementations en vigueur ainsi que les normes et standards reconnus de l'industrie en la matière. Le Client se réserve le droit d'imposer en tout temps ses propres méthodes ou procédures de destruction.

6.3. Sur demande du Client, le Fournisseur doit fournir immédiatement des preuves de destruction de l'Information du Client et toutes informations relatives aux méthodes ou procédures de destruction utilisées.

7. ANONYMISATION DE L'INFORMATION DU CLIENT

7.1. Le Client peut à tout moment ordonner au Fournisseur d'anonymiser toutes Informations du Client dans un délai raisonnable. Toute anonymisation doit être réalisée selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement et par la Loi.

7.2. Sur demande du Client, le Fournisseur doit fournir immédiatement des preuves d'anonymisation de l'Information du Client et toutes informations relatives aux méthodes ou procédures utilisées.

8. TRAITEMENT DES INFORMATIONS DU CLIENT ET CONTRÔLE DES ACCÈS

8.1. Sauf instruction contraire écrite du Client, le Fournisseur s'engage à ne Traiter les Informations du Client que conformément à l'Entente et à ses Annexes et qu'aux fins nécessaires à son exécution. Les employés, sous-traitants ou mandataires, ne peuvent accéder aux Informations du Client que si cela est nécessaire à l'exercice des obligations prévues par l'Entente et ses Annexes.

8.2. Le Fournisseur doit limiter l'accès de ses employés, sous-traitants ou mandataires aux systèmes utilisés et à l'Information du Client dans le cadre de l'exécution des obligations prévues par l'Entente en mettant en œuvre un processus de gestion des accès et du Traitement de l'Information du Client ainsi que des mesures d'authentification (par ex. authentification multifacteurs, authentification unique, etc.) (ci-après « **Contrôle des accès** »). Ce Contrôle des accès doit être conforme aux Lois sur la protection des renseignements personnels et aux normes et standards reconnus dans le domaine de la sécurité informatique et de la gestion des accès logiques et physiques.

8.3. Le Fournisseur doit gérer les accès et le Traitement de l'information en assurant l'imputabilité des actions liées aux accès en tout temps, en utilisant les principes du besoin de savoir et du moindre privilège d'accès, et en prenant les actions appropriées en temps opportun lors de la modification des responsabilités d'un de ses employés, sous-traitants ou mandataires. De plus, des moyens matériels, des mécanismes organisationnels et des mécanismes techniques doivent être mis en place pour assurer une séparation des tâches (ex. : assignation de privilèges d'accès en fonction des tâches). Lorsque la séparation des tâches ne peut être mise en place, des contrôles compensatoires doivent être mis en œuvre (ex. : revue régulière des journaux d'activités) et le Fournisseur doit en informer le Client. Le Fournisseur doit effectuer une revue des accès et des privilèges annuellement afin de s'assurer que les accès de ses employés, sous-traitants ou mandataires respectent les principes du besoin de savoir et du moindre privilège d'accès et que les accès inutilisés, pendant plus d'un mois, sont désactivés.

8.4. Le Fournisseur doit retirer, dans un délai de vingt-quatre (24) heures de la fin de l'implication ou de début d'une absence prolongée d'un employé, sous-traitant ou mandataire, les accès de ce dernier à l'Information du Client.

9. ACCÈS À DISTANCE

9.1. Sans limiter ses autres obligations en vertu de la présente Annexe de sécurité, le Fournisseur doit définir et implémenter des politiques de sécurité sur les accès à distance aux Informations du Client par ses employés, mandataires et sous-traitants. Sans s'y limiter, le Fournisseur doit :

(a) définir un code de conduite et une politique sur le Télétravail et s'assurer que ses employés, sous-traitants et mandataires s'y conforment ;

(b) s'assurer que les données du Client ne peuvent pas être copiées sur des supports amovibles, téléchargées ou imprimées en lot ;

(c) mettre en place une authentification multifacteurs pour les connexions ;

(d) s'assurer que ses employés utilisent des postes de travail contrôlés et endurcis selon les meilleures pratiques de l'industrie ; et

(e) mettre en place des mécanismes de surveillance sur les accès aux informations du Client.

10. MESURES DE SÉCURITÉ

10.1. Le Fournisseur doit mettre en œuvre des processus de journalisation et de surveillance des systèmes informatiques afin de permettre la détection et le signalement d'anomalies et de permettre une intervention rapide. Ces processus et systèmes doivent être conformes aux normes et standards reconnus de l'industrie en matière de sécurité de l'information.

10.2. Le Fournisseur doit implémenter des mécanismes de protection contre le vol de données pour identifier, détecter et surveiller les actions de ses employés et Agents sur les Informations du Client.

10.3. Le Fournisseur doit définir et mettre en œuvre des mesures de prévention, de détection et de récupération pour se protéger contre les logiciels malveillants. De plus, le Fournisseur doit installer un logiciel pour détecter les logiciels malveillants sur les équipements informatiques qu'il utilise pour le Traitement de l'Information du Client. Le Fournisseur doit opter pour le service de mise à jour automatique proposé par son fournisseur de logiciels de protection contre les logiciels malveillants.

10.4. Le Fournisseur doit, à ses frais, tester la sécurité des systèmes, des infrastructures et des applications qu'il utilise pour l'exploitation de sa solution technologique. Ces tests doivent être

effectués par du personnel qualifié et doivent se conformer aux normes et standards reconnus de l'industrie. Le Client se réserve le droit de demander des modifications à la méthodologie et la portée de ces tests.

10.5. Le Fournisseur doit définir et mettre en œuvre un processus de gestion des correctifs et des vulnérabilités, basé sur les normes et standards reconnus dans ce domaine. Le Fournisseur doit utiliser exclusivement des infrastructures, des technologies et des logiciels qui sont supportés et recommandés par les normes et standards reconnus de l'industrie en matière de sécurité de l'information. Le Fournisseur doit prendre les actions appropriées pour prévenir l'exploitation d'une vulnérabilité entre le moment qu'elle a été déclarée ou détectée et le moment que le correctif est appliqué. Le Fournisseur doit divulguer immédiatement toute vulnérabilité au Client et corriger celle-ci dans les plus brefs délais.

10.6. Le Fournisseur doit mettre en place des mécanismes conformes aux normes et standards reconnus de l'industrie pour protéger l'Information du Client. Sans s'y limiter, le Fournisseur doit s'assurer que l'Information du Client est chiffrée en transit et au repos conformément aux normes et standards de l'industrie. Les Informations du Client doivent être en tout temps adéquatement protégées contre toutes interceptions, leurs copies, modifications ou destructions non autorisées. Les données en transit doivent être protégées par les protocoles de communication sécuritaires standardisés et reconnus dans l'industrie.

10.7. Le Fournisseur doit mettre en place un processus de gestion cryptographique basé sur les normes et standards reconnus de l'industrie pour sa gestion des clés de chiffrement.

11. GESTION DES TIERS

11.1. Le Fournisseur ne peut pas sous-traiter ou mandater un tiers dans l'exécution de la présente Entente sans l'approbation écrite du Client.

11.2. Le Fournisseur doit informer le Client par écrit, au moins un mois à l'avance, de son intention de faire affaire avec un Agent en indiquant l'identité de celui-ci, sa juridiction, l'endroit où les Informations du Client seront Traitées et les opérations de traitement concernées.

11.3. Le Fournisseur doit mettre en place un processus de vérification et de gestion des tiers dans le but d'assurer que les exigences de sécurité formulées par la présente Entente sont respectées par ses Agents. Le processus doit inclure, sans s'y limiter, l'évaluation et la surveillance des mesures de sécurité implémentées par ses sous-traitants et mandataires. Sur demande, le Fournisseur doit communiquer au Client toutes informations se rapportant à ces vérifications.

11.4. Sauf instruction contraire du Client, le Fournisseur doit s'assurer que son entente avec son Agent prohibe toute communication ou tout transfert des Informations du Client à un tiers. Elle doit également prohiber tout traitement des Informations du Client qui serait incompatible avec les obligations stipulées par l'Entente, par ses Annexes ou par les Lois sur la protection des renseignements personnels. Cette entente doit également prévoir que le sous-traitant ou mandataire doit transférer (au Client ou au Fournisseur) et détruire les Informations du Client dès que le Client ou le Fournisseur en formule la demande.

11.5. Le Client peut à tout moment, sans motif, exiger que le Fournisseur cesse d'utiliser les services d'un sous-traitant ou d'un mandataire dans le cadre de l'exécution de l'Entente.

11.6. Le Fournisseur demeure en tout temps responsable des actes et omissions de ses Agents.

12. GESTION DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

12.1. Pour les fins de la présente Annexe de sécurité, l'expression « Incident de sécurité » se manifeste lors de l'une des situations suivantes :

(a) une atteinte ou violation, réelle ou présumée, à la sécurité ou à la protection de l'Information du Client ou d'une disposition de la présente Annexe de sécurité ou de l'Annexe de PRP;

(b) un Incident de confidentialité tel que défini par l'Annexe de PRP ; et

(c) tout évènement de sécurité pouvant avoir un impact soupçonné ou confirmé sur l'Information du Client.

12.2. Le Fournisseur doit définir et mettre en œuvre un processus et des procédures de gestion des Incidents de sécurité de l'information. Ce processus doit être basé sur les normes et standards reconnus dans le domaine de la gestion des incidents liés à la sécurité de l'information.

12.3. Le Fournisseur doit tester au moins une fois par année son plan de réponse aux incidents de sécurité de l'information et, à la demande du Client, communiquer les résultats.

12.4. Lorsqu'un Incident de sécurité est soupçonné ou confirmé, le Fournisseur doit immédiatement signaler l'incident au Responsable de la protection des renseignements personnels du Client. Il doit signaler l'incident par téléphone puis par courriel marqué des mentions « haute importance » et « suivi immédiat ».

12.5. Ce signalement, dans la mesure du possible et selon la situation, devra contenir les informations suivantes : les circonstances et la nature de l'Incident de sécurité, la date et l'heure de l'Incident de sécurité, la date et heure de sa détection ainsi que le nom et les coordonnées du point de contact du Fournisseur auprès duquel des informations supplémentaires pourraient être obtenues. Si l'Incident de sécurité constitue un Incident de confidentialité au sens de l'Annexe de PRP, le signalement doit également contenir les informations prévues à l'article 8.3 de l'Annexe de PRP.

12.6. Suite à l'Incident de sécurité, et après consultation auprès du Client, le Fournisseur s'engage à mettre tous les moyens raisonnables pour :

(a) remédier promptement à l'évènement ;

(b) prendre les mesures et stratégies nécessaires qui permettront d'éviter que l'évènement ne se reproduise ;

(c) minimiser tout dommage réel ou potentiel subi par le Client ;

(d) si l'évènement constitue un Incident de confidentialité, remédier promptement à l'évènement et minimiser tout dommage potentiel et qui pourrait être subit par les personnes concernées par les renseignements personnels touchés par l'Incident de confidentialité ;

(e) si l'évènement constitue un Incident de confidentialité, il doit inscrire l'évènement à son registre d'Incidents de confidentialité selon les modalités prévues à l'article 8.3 de l'Annexe de PRP ;

(f) entreprendre une enquête approfondie sur les causes de l'Incident de sécurité ; et

(g) suivre toute instruction du Client, notamment en ce qui concerne les mesures de remédiation découlant de l'Incident de sécurité ou les mesures conservatoires à mettre en place pour éviter tout autre Incident de sécurité.

12.7. Un rapport post-mortem doit être communiqué au Client cinq (5) jours ouvrables après la résolution de l'Incident, contenant notamment :

(a) les causes racines de l'Incident ;

(b) les actions qui ont été entreprises pour résoudre l'Incident ;

(c) un Plan d'action pour éviter la répétition de l'Incident; et

(d) un Échéancier de la mise en œuvre des mesures prévues par le plan d'action.

12.8. Le Fournisseur doit permettre au Client et à son Responsable de la protection des renseignements personnels de réaliser toutes vérifications en lien avec l'évènement et la confidentialité des Informations concernées qu'il estime nécessaire. Le Client pourra, à sa discrétion, demander des modifications au Plan d'action ou à l'Échéancier ou imposer un nouveau Plan d'action et Échéancier.

12.9. Toutes les actions entreprises dans le cadre de la gestion des Incidents de sécurité de l'information sont à la charge du Fournisseur.

12.10. Le Fournisseur communiquera régulièrement avec le Client pour l'informer des développements de l'enquête et du plan d'action relative à l'Incident de sécurité et coopérera pour fournir toute information requise supplémentaire ou demandée par le Client en temps opportun. Sous réserve des lois applicables, et afin d'assurer une communication cohérente et appropriée, le Fournisseur obtiendra le consentement écrit du Client avant d'informer un tiers de l'Incident de sécurité. Le Fournisseur doit obtenir l'autorisation écrite du Client avant de faire référence au Client dans toute communication externe portant sur les Incidents de sécurité.

13. CONFORMITÉ ET AUDIT

13.1. Le Client se réserve aux frais du Fournisseur le droit de procéder ou de faire procéder par son mandataire à tout moment à un audit chez le Fournisseur, afin de s'assurer que l'exécution des obligations prévues par l'Entente soit conforme aux dispositions de la présente Annexe de sécurité et de l'Annexe de PRP.

13.2. Le Fournisseur doit mettre à la disposition du Client et à la demande de ce dernier, toute information nécessaire afin de démontrer la conformité du Fournisseur avec la présente Annexe de sécurité et l'Annexe de PRP.

13.3. Le Fournisseur doit coopérer et contribuer aux audits et contrôles effectués par le Client ou par un auditeur mandaté par le Client.

13.4. Sous réserve d'un préavis communiqué au Fournisseur, le Client ou un auditeur mandaté par le Client peut, à tout moment, pénétrer les locaux ou lieux dans lesquels les Renseignements personnels sont traités. Le Client ou un auditeur mandaté par le Client peuvent consulter, contrôler, vérifier ou copier tout dossier pertinent, tout processus ou tout système, afin d'en vérifier la conformité avec l'Entente et ses Annexes et avec les Lois sur la protection des renseignements personnels.

13.5. Advenant que des non-conformités soient constatées par le Client, le Fournisseur devra les corriger, à ses frais, selon un Plan d'action et un Échéancier approuvés par le Client.

13.6. À la demande du Client, le Fournisseur doit déposer des preuves que les plans d'action ont été adéquatement mis en œuvre.

13.7. Le Client n'a pas le devoir de faire cet audit et le Client n'engage pas sa responsabilité s'il décide de faire, ou de ne pas faire une telle visite, inspection, examen, audit ou vérification. Le Client n'engage pas non plus sa responsabilité pour tout manquement ou toutes violations qui n'auraient pas été détectées par l'audit.

14. AMENDEMENT

14.1. Le Client peut décider, à son entière discrétion, de modifier la présente Annexe de sécurité afin, entre autres, d'y introduire, d'y modifier ou d'y éliminer des obligations, des pratiques, des mesures ou des procédures afin d'assurer la conformité du Fournisseur, la conformité d'un Sous-traitant ou la conformité du Client aux exigences légales ou réglementaires. Pour ce faire, le Client doit préalablement envoyer un avis écrit au Fournisseur qui identifie le motif de la modification et les modifications imposées.

15. SURVIE

15.1. Dans la mesure où le Fournisseur continue d'avoir accès ou contrôle à des Informations du Client pour quelque raison que ce soit, le Fournisseur continuera à être lié par les termes de la présente Annexe de sécurité.

SIGNÉ À _____, ce _____

SADC d'Antoine-Labelle	**[ ]**
(FOURNISSEUR)	**(CLIENT)**
Par : _____	Par : _____
Nom du Représentant	Nom du Représentant
Titre du Représentant	Titre du Représentant
Signature du Représentant	Signature du Représentant