Le présent document (la présente « **annexe** ») est l'annexe relative aux services ONE Network (« **services ONE Network** »), comme définie ci-dessous, faite en application de la convention relative aux services de cyberSanté Ontario (la « **convention** ») passée entre cyberSanté Ontario et le client mentionné ci-dessous (le « **client** »), datée le **<effective date of SA : MMMM, dd, yyyy>** et entrant en vigueur le **<this schedule signing date : MMMM, dd, yyyy>** (la « **date d'entrée en vigueur** »). Les services ONE Network seront fournis par cyberSanté Ontario lors de l'acceptation par le client des modalités de la présente annexe et de la confirmation écrite de cyberSanté Ontario que cette annexe signée a été reçue et acceptée.

Dénomination sociale du client

<Insérer la dénomination sociale, une société constituée aux termes de [nom de la loi]>

1. Définitions

Sauf mention contraire dans la présente annexe, les termes définis dans celle-ci ont le sens qui leur a été attribué dans la convention :

« Systèmes du client » signifient les systèmes informatiques, les périphériques, les terminaux, l'équipement de communication et la totalité du matériel connexe dont le client est propriétaire ou locataire et qui sera utilisé par celui-ci en relation avec son utilisation des services ONE Network;

« **Application informatique** » signifie tout logiciel dont le client est propriétaire ou pour lequel il détient une licence d'utilisation, qu'il utilise à des fins commerciales légitimes et relativement avec son utilisation des services ONE Network;

« **Formulaire de client du réseau ONE Network** » signifie le formulaire rempli conjointement par le client et cyberSanté Ontario et qui contient les coordonnées et les renseignements techniques nécessaires à l'utilisation des services ONE Network par le client;

« Services ONE Network » signifie les services fournis au client par cyberSanté Ontario afin de se connecter à l'infrastructure technologie de cyberSanté Ontario et à tout service connexe par l'entremise du réseau privé géré qui est exploité par cyberSanté Ontario (« **réseau ONE Network** »), comme décrit dans l'article 2 ci-dessous, et

« **équipement lié au service** » signifie tout équipement ou logiciel pouvant être sélectionné par cyberSanté Ontario (ou par tout représentant de cyberSanté Ontario) et fourni au client relativement aux ONE Network, y compris les pare-feu, les routeurs, les commutateurs, les convertisseurs de médias, les modems, les câbles, les câbles à fibre optique, les panneaux, les ordinateurs de bureau, les ordinateurs portables, les serveurs, les armoires, les alimentations sans coupure, les terminaux serveurs et les jetons matériels, mais sans inclure tout équipement acheté par le client.

2. Services ONE Network

2.1 **Prestation des services.** Lorsqu'il demande les services ONE Network, le client devrait remplir le formulaire de client du réseau ONE Network et remplir, signer et soumettre la présente annexe. La prestation des services ONE Network au client est assujettie aux modalités de la convention, y compris la présente annexe et ses pièces, ainsi qu'à la confirmation de cyberSanté Ontario qu'il peut fournir les services ONE Network. Aucune propriété dans les services ONE Network n'est transférée au client en vertu de la présente annexe et le client ne possède que le droit limité d'accéder aux services, comme énoncé dans la présente annexe.

2.2 **Services ONE Network.** Chaque partie fournira à l'autre partie les renseignements raisonnablement demandés relativement aux services ONE Network. Le client reconnaît que les services ONE Network lui sont fournis pour sa propre utilisation et non pour l'utilisation par une autre organisation ou personne. Le client ne permettra à aucune autre personne ou organisation d'utiliser les services ONE Network.

2.3 **Obligations du client.** Le client convient de fournir un environnement approprié et sécurisé pour permettre à cyberSanté Ontario d'installer et de localiser l'équipement lié au service, ainsi qu'un accès raisonnable au site pour livrer, installer, entretenir, inspecter, débrancher ou enlever l'équipement lié au service. Le client assumera les coûts liés à l'infrastructure locale pour l'interface avec l'équipement lié au

service et l'utilisation de celui-ci, et il veillera à ce que tout équipement lié au service se trouvant dans ses locaux soit protégé contre le risque de perte ou de dommages, dans un environnement qui respecte les spécifications du fabricant. Le client assumera la responsabilité de la perte et des risques de dommages à l'équipement lié au service, sauf lorsque cela est causé par la négligence ou l'inconduite volontaire de cyberSanté Ontario, et lors de la résiliation des services ONE Network (quelle qu'en soit la raison), le client accepte de renvoyer tout l'équipement lié au service à cyberSanté Ontario.

2.4 **Équipement du client et locaux.** Le client assumera les coûts et la responsabilité liés à l'obtention, l'acquisition et l'installation de l'infrastructure dont il pourrait avoir besoin pour accéder aux services ONE Network et les utiliser, y compris l'équipement, les logiciels, les câbles, les conduits, l'électricité, les systèmes de chauffage ou de refroidissement, les conduites d'entrée, les baies et les étagères. Pour permettre à cyberSanté Ontario de s'acquitter de ses obligations en vertu de la présente annexe, le client obtiendra (à ses frais) les droits et les autorisations nécessaires pour permettre à cyberSanté Ontario d'accéder à tout équipement ou logiciel utilisé par le client relativement aux services ONE Network et à se connecter à ceux-ci. Le client fournira à cyberSanté Ontario un accès raisonnable à ses locaux, afin de permettre à cyberSanté Ontario de s'acquitter de ses responsabilités ou d'exercer ses droits en vertu de la présente annexe. Lorsqu'il est présent dans les locaux du client, cyberSanté Ontario respectera, et fera en sorte que ses représentants respectent également, les politiques raisonnables concernant l'accès et la sécurité communiquées par écrit par le client.

2.5 **Équipement lié au service.** cyberSanté Ontario peut remplacer ou modifier toute pièce d'équipement lié au service, tant que cela n'a pas d'effet négatif important sur les services ONE Network. L'équipement lié au service reste la propriété de cyberSanté Ontario ou de ses représentants, et le client n'obtiendra aucun intérêt sur l'équipement lié au service et ne doit ni déposer ni permettre l'existence de liens ou d'autres charges sur celui-ci.

2.6 **Changements aux services.** cyberSanté Ontario peut, à son entière discrétion, modifier ou moderniser l'infrastructure utilisée par cyberSanté Ontario pour fournir les services ONE Network de temps à autre. Le client assume exclusivement la responsabilité de la modification ou de la mise à jour des systèmes du client ou des applications informatiques causées par la modification ou la mise à jour de l'infrastructure utilisée par cyberSanté Ontario pour fournir les services ONE Network.

2.7 **Engagement relatif aux niveaux de service.** cyberSanté Ontario fera des efforts commercialement raisonnables pour fournir les services ONE Network et ne prend aucun engagement relatif aux niveaux de service dans la présente annexe ou relativement avec les services ONE Network.

2.8 **Soutien.** cyberSanté Ontario fournira au client un soutien et une aide techniques concernant les services ONE Network, par l'entremise d'un service de dépannage disponible par téléphone. cyberSanté Ontario peut changer le numéro de téléphone applicable de temps à autre. cyberSanté Ontario ne garantit pas qu'il sera en mesure de vérifier ou de résoudre tous les problèmes présentés au service de dépannage par le client. Le client reconnaît que c'est lui, et non cyberSanté Ontario, qui est exclusivement responsable de résoudre tout problème avec sa propre infrastructure technologique et de maintenir l'exactitude des renseignements figurant dans le formulaire de client du réseau ONE Network.

2.9 **Descriptions en langage simple.** Le client reconnaît avoir reçu de la part de cyberSanté Ontario les descriptions en langage simple des services ONE Network, y compris une description des mesures de protection relatives à ceux-ci. L'exemplaire en vigueur des descriptions en langage simple est jointe à la présente annexe en tant que pièce A et est également disponible en ligne à www.ehealthontario.on.ca/fr/services/one-network. cyberSanté Ontario peut modifier les descriptions en langage simple de temps à autre, conformément à la convention.

2.10 **Politiques.** Le client reconnaît avoir reçu de la part de cyberSanté Ontario la politique d'utilisation acceptable et la politique de sécurité relatives à l'utilisation des services ONE Network. Les copies en vigueur de la politique d'utilisation acceptable et de la police de sécurité sont jointes à la présente annexe en tant que pièce B et pièce C respectivement, et sont également disponibles en ligne à l'adresse www.ehealthontario.on.ca/fr/services/one-network cyberSanté Ontario peut modifier ces politiques de temps à autre, conformément à la convention.

3. Vérification

Le client autorise cyberSanté Ontario et ses représentants, sur remise d'un préavis de cinq (5) jours et pendant les heures de bureau, à inspecter les dossiers et les documents qui sont en la possession ou sous le contrôle du client et relatives aux responsabilités de celui-ci comme prévu en vertu de la présente annexe. cyberSanté Ontario peut exercer ses droits en vertu du présent article 3 afin de vérifier la conformité avec les modalités de la présente annexe et toute condition applicable de la convention.

4. Durée et résiliation

4.1 **Durée**. La présente annexe commence à la date d'entrée en vigueur et est maintenue, sauf si elle est résiliée conformément aux articles 4.2 ou 4.3.

4.2 **Résiliation à des fins de commodité**. Chacune des parties peut, à son entière discrétion, sans obligation, coût ou pénalité et sans porter atteinte à tout autre droit ou recours en vertu de la présente annexe, légalement ou en equity, résilier la présente annexe à n'importe quel moment sur remise d'un préavis écrit d'au moins quatre-vingt-dix (90) jours à l'autre partie.

4.3 **Suspension.** cyberSanté Ontario aura le droit de suspendre immédiatement la prestation du service ONE Network s'il estime raisonnablement qu'une telle mesure est justifiée par une situation d'urgence ou par les circonstances.

4.4 **Résiliation de la convention**. La présente annexe prend fin automatiquement sans obligation, coût ou pénalité, et sans porter atteinte à tout autre droit ou recours à la disposition de cyberSanté Ontario en vertu de la présente annexe, de la convention, légalement ou en equity, si la convention expire ou est résiliée pour quelque raison que ce soit.

4.5 **Effet de la résiliation**. Le client reconnaît que lors de la résiliation de la présente annexe, tout accès aux services ONE Network sera révoqué.

4.6 **Survie**. Dans l'éventualité de l'expiration ou de la résiliation de la présente annexe pour quelque raison que ce soit, les articles 4.4, 4.5 et 5 survivront.

5. Limitation de responsabilité

5.1 **Limitation.** Sauf mention contraire expresse dans la présente annexe, en aucun cas une partie ne sera tenue responsable des pertes, des dépenses ou des dommages indirects, consécutifs, accessoires, punitifs ou exemplaires, ni de la perte de données, de revenus ou de profits, même si elle a été informée de leur possibilité ou s'ils étaient raisonnablement prévisibles. La responsabilité d'une partie envers l'autre partie en ce qui concerne l'exécution ou la non-exécution ou pour toute question relative à la présente annexe ou à la convention, pour la totalité des réclamations, ne dépassera pas au total le plus élevé des montants suivants :

(i) 250 000 $ ou

(ii) 5 000 $ multiplié par le nombre d'enregistrements de toute personne inscrite dans un service parrainé lancé ou complété par un représentant du client.

Cette limite s'appliquera sans tenir compte de la nature de la cause d'action, de la demande ou de la réclamation, y compris une violation de contrat, la négligence, le tort ou toute autre théorie juridique.

5.2 **Déni de responsabilité.** cyberSanté Ontario nie expressément les assertions, les garanties ou les conditions relatives aux services ONE Network décrits dans la présente annexe ou en découlant, qu'ils soient explicites ou implicites, passés ou présents, prescrits par la loi ou autres, y compris, notamment, toute garantie implicite ou condition de qualité marchande ou d'adaptation à un usage particulier.

6. Dispositions générales

Intégralité de l'entente. À l'exception de la convention et de tout autre document qui lui est joint ou qui fait mention de présente annexe, la présente annexe constitue l'intégralité de l'entente entre les parties relativement au sujet des présentes et elle remplace la totalité des ententes, des négociations et des discussions antérieures, écrites ou verbales, entre les parties. Les parties reconnaissent et conviennent

que la signature de la présente annexe n'a pas été incitée par des assertions ou des écrits qui ne sont pas incorporés à la présente annexe afin d'en faire partie, et ni l'une ni l'autre des parties n'a compté sur de telles assertions ou de tels écrits ou les a considérés comme étant importants. La présente annexe inclut les pièces et les pièces jointes suivantes, le cas échéant :

(a) Pièce A : Descriptions en langage simple;
(b) Pièce B : Politique d'utilisation acceptable; et
(c) Pièce C : Politique de sécurité.

Pièce A – Description en langage simple

1. Services de réseau. ONE Network permet aux fournisseurs de soins de santé d'échanger des renseignements en toute confiance par l'entremise d'un réseau haute vitesse construit pour les soins de santé. Lorsque cyberSanté Ontario fournit les services ONE Network au client, il fournit un ou plusieurs circuits de télécommunication au Ontario, faisant en sorte qu'un ou plusieurs réseaux sous le contrôle du client sont connectés à l'infrastructure technologique de cyberSanté Ontario. Un circuit peut être basé sur différentes technologies, par exemple une ligne d'abonné numérique, un câble, un satellite ou un câble à fibre optique.

2. Sécurité et mesures de protection de la vie privée.

2.1 Tous les produits et services de cyberSanté Ontario :
Le programme de sécurité de cyberSanté Ontario est fondé sur deux normes de l'Organisation internationale de normalisation (ISO) recommandées par le gouvernement du Canada :

- ISO/IEC 27002:2005, – Code de bonne pratique pour le management de la sécurité de l'information, et
- ISO/IEC 27001:2005, – Systèmes de management de la sécurité de l'information – Exigences.

et il respecte la *Loi sur la protection des renseignements personnels sur la santé* et la *Loi sur l'accès à l'information et la protection de la vie privée*. La sécurité de l'information et la protection de la vie privée dans le cadre des produits et des services de cyberSanté Ontario, ainsi que leur utilisation, sont réalisées grâce à la collaboration de toutes les parties qui sont des partenaires dans la prestation ou l'utilisation de ces services. Pour sa part, cyberSanté Ontario a mis en œuvre les mesures de protection suivantes :

(i) Mesures de protection administratives

- cyberSanté Ontario examine et améliore régulièrement ses politiques de sécurité. Les employés et les entrepreneurs lisent les politiques pertinentes et signent pour confirmer qu'ils les ont lues et comprises.
- cyberSanté Ontario a mis en œuvre des programmes obligatoires de sensibilisation et de formation du personnel de sécurité.
- En général, ni les employés ni les entrepreneurs de cyberSanté Ontario n'ont la capacité ou la permission d'accéder aux renseignements personnels sur la santé. Si un accès aux renseignements personnels sur la santé est requis dans le cadre de la prestation des services de cyberSanté Ontario, il est interdit d'utiliser ou de divulguer de tels renseignements.
- Tous les employés et les entrepreneurs doivent signer des ententes de confidentialité et subir une vérification de leur casier judiciaire avant d'entrer au service de cyberSanté Ontario. cyberSanté Ontario a mis en place une procédure de contrôle de sécurité qui nécessite que les employés aient un niveau d'autorisation approprié à la sensibilité des renseignements auxquels ils accèdent.
- Les obligations du client relatives au maintien de la sécurité sont décrites dans des contrats individuels et dans des ententes sur les niveaux de service (ENS).
- Par l'entremise de contrats ou d'ENS officiels, cyberSanté Ontario veille à ce que tout tiers qu'il embauche pour l'aider à fournir des services à des gardiens de renseignements sur la santé respectent les restrictions set les conditions nécessaires pour que cyberSanté Ontario puisse s'acquitter de ses obligations légales.
- Les employés, les consultants, les fournisseurs et les clients de cyberSanté Ontario doivent signaler dans les plus brefs délais à cyberSanté Ontario toute atteinte à la sécurité afin qu'une enquête puisse être menée.
- Des évaluations des risques liés à la sécurité ont lieu dans le cadre du développement de produits ou de services et de déploiements chez les clients. Les activités d'atténuation sont bien établies et leur suivi est assuré dans le cadre de chaque évaluation.
- cyberSanté Ontario fournit une copie écrite des résultats d'une évaluation des risques liés à la sécurité aux gardiens affectés des renseignements sur la santé.
- cyberSanté Ontario a établi un programme officiel de gestion des risques, y compris une politique et des lignes directrices relatives à la gestion des risques pour l'entreprise.
- cyberSanté Ontario effectue régulièrement des évaluations indépendantes de la vulnérabilité des configurations techniques et des pratiques de sécurité opérationnelles.

(ii) Mesures de protection technologiques

- Pour obtenir un accès aux systèmes sensibles, des mots de passe forts, des jetons sécurisés et d'autres authentifiants sont requis.
- L'accès administratif à tout l'équipement informatique est contrôlé par l'entremise d'une authentification forte à deux facteurs et cet accès est consigné.
- cyberSanté Ontario surveille et gère le trafic réseau en utilisant des mécanismes de sécurité tels que des routeurs, des commutateurs, des pare-feu de réseau, des systèmes de détection des intrusions et des logiciels antivirus.
- cyberSanté Ontario crypte toutes les données stockées sur les ordinateurs de ses employés.

(iii) Mesures de protection physiques

- Les centres de données de cyberSanté Ontario sont construits sur mesure et protégés physiquement contre les accès non autorisés, et dotés de personnel de sécurité en permanence qui les surveille constamment.
- Les mesures de contrôle de la sécurité physique des centres de données ont été validées par un tiers indépendant, conformément aux normes du gouvernement fédéral.
- cyberSanté Ontario exige une escorte en tout temps pour les fournisseurs tiers et le personnel d'entretien qui doivent avoir accès au centre de données.

2.2 Mesures de protection du réseau ONE Network. En plus des mesures de protection génériques qui s'appliquent à tous les produits et services de cyberSanté Ontario, les mesures de sécurité suivantes sont en place pour le réseau ONE Network :

- Le trafic de cyberSanté Ontario sur le réseau ONE Network est séparé d'Internet et est protégé par une approche de défense en profondeur contre les menaces provenant de réseaux externes.
- Les clients doivent prendre des mesures appropriées pour séparer leurs propres réseaux internes contre des réseaux non fiables.
- L'équipement du réseau ONE Network est déployé en vue d'une utilisation exclusive par cyberSanté Ontario afin de fournir le service ONE Network, et il est exploité conformément aux pratiques et aux politiques de cyberSanté Ontario.
- Le réseau ONE Network est mis à l'œuvre à l'échelle de la province. Il a recours à des liens dédiés par fibre optique et à des réseaux de transporteurs tiers.
- Le cryptage utilisant des tunnels IPSec sur des réseaux de transporteurs tiers permet d'assurer la sécurité des communications de cyberSanté Ontario qui traversent ces réseaux.
- Tous les clients signent des ententes attestant qu'ils s'assureront que l'équipement du réseau ONE Network se trouvant dans leurs locaux est installé dans des environnements physiquement sécurisés, qui seront contrôlés et surveillés.
- cyberSanté Ontario a mis en œuvre un programme complet de gestion de la sécurité d'entreprise et des incidents d'atteinte à la vie privée.
- Tous les changements apportés au réseau sont contrôlés par cyberSanté Ontario et font l'objet de ses pratiques officielles de gestion des changements.
- Le personnel administratif n'a aucun accès aux données de cyberSanté qui circulent sur le réseau ONE Network.
- cyberSanté Ontario peut séparer les communications entre certains sites clients (p. ex., pour des bureaux géographiquement séparés).
- Chaque point d'accès au réseau est doté de mesures de contrôle permettant de protéger le réseau contre les menaces pour la sécurité, qu'elles soient malicieuses ou accidentelles.

Pièce B – Politique d'utilisation acceptable

1. Résumé

La présente politique définit les critères d'utilisation acceptable des produits et services de cyberSanté Ontario, ainsi que l'infrastructure technologique utilisée par cyberSanté Ontario pour fournir ces produits et services. cyberSanté Ontario peut réviser cette politique lorsqu'il le juge utile. Toute révision sera affichée sur le site http://www.ehealthontario.on.ca/fr/services/one-network. Vous serez avisé des révisions conformément à l'entente en vertu de laquelle cyberSanté Ontario vous fournit des produits ou des services.

2. Portée et application

La présente politique s'applique à tous les utilisateurs. Toute personne qui a accès à l'infrastructure technologique, qui se sert de cette infrastructure ou qui utilise un produit ou service fourni par cyberSanté Ontario constitue un « utilisateur ». Le terme « personne » désigne un particulier, une personne, une succession, une fiducie, une entreprise, une société de personnes ou une société, un gouvernement, un organisme gouvernemental ou un ministère ainsi qu'un successeur de ceux-ci.

3. Responsabilité

Chaque organisme client est responsable de l'accès aux produits, aux services ou à l'infrastructure technologique de cyberSanté Ontario ainsi qu'à leur utilisation par tout utilisateur qui est un particulier et qui a obtenu, de cet organisme client ou sur les instructions de cet organisme client, ses mots de passe, ses jetons sécurisés, ses certificats numériques et tout autre identifiant (« **justificatifs d'identité** ») lui permettant d'accéder à l'infrastructure technologique et à tout produit ou service fourni par cyberSanté Ontario.

4. Utilisation acceptable

Les utilisateurs ne sont autorisés à utiliser les produits, les services et l'infrastructure technologique de cyberSanté Ontario que pour des activités liées à la santé.

5. Utilisations inappropriées et inacceptables

Les utilisateurs ne doivent pas utiliser les produits, les services ou l'infrastructure technologique de cyberSanté Ontario d'une manière inappropriée ou inacceptable. Entre autres, ils ne doivent pas :

a) Créer, recueillir, transmettre, entreposer ou échanger du matériel en violation des lois applicables;

b) Se livrer à de la diffamation (répandre de fausses allégations ou des rumeurs au sujet des autres, par exemple);

c) Accéder à de l'information ou l'utiliser, la recueillir, la détruire, la crypter, la modifier ou l'éliminer en violation des lois applicables;

d) Fabriquer, posséder ou distribuer des programmes informatiques conçus pour aider à obtenir l'accès à des systèmes informatiques en violation des lois applicables;

e) Promouvoir la haine contre un groupe ou une personne identifiable en communiquant de l'information en violation des lois applicables;

f) Harceler d'autres personnes par voie électronique (faire des menaces concernant la sécurité ou les biens d'une personne, par exemple);

g) Posséder, visionner, télécharger, transmettre ou entreposer du matériel pornographique ou participer d'une manière quelconque au trafic de ce type de matériel;

h) Utiliser le mot de passe, le jeton sécurisé, les certificats numériques ou tout autre identifiant d'une autre personne afin de se livrer à des activités en violation des lois applicables;

i) Violer le droit d'auteur, un secret commercial ou tout autre droit de propriété intellectuelle (violer des licences d'utilisation de logiciels, pirater de la musique enregistrée ou des films ou voler des secrets commerciaux, par exemple);

j) Contourner volontairement les dispositifs de protection physiques, logiques ou procéduraux de cyberSanté Ontario, notamment les pare-feu, les filtres Web ou d'autres dispositifs de contrôle d'accès;

k) Se livrer à un acte de vandalisme, qui est défini comme une tentative de porter atteinte à de l'information d'un autre utilisateur ou à de l'information contenue sur Internet ou sur d'autres réseaux, ou de détruire cette information;

l) Se livrer à du harcèlement, ce qui consiste notamment à avoir des contacts non professionnels persistants avec un autre utilisateur, lorsque de tels contacts ne sont pas sollicités, ou à empoisonner le climat de travail en accédant à du contenu offensant ou encore en affichant, en sauvegardant, en téléchargeant ou en transmettant un tel contenu;

m) Envoyer des courriels non désirés ou des documents commerciaux ou publicitaires non sollicités à une autre personne;

n) Accéder de façon délibérée et non autorisée à de l'information, à des installations ou à des services accessibles au moyen de l'infrastructure de cyberSanté Ontario;

o) Utiliser, recueillir, éliminer, détruire, crypter, modifier ou divulguer sans autorisation des renseignements personnels, des secrets commerciaux ou des renseignements sensibles fournis par ou obtenus de cyberSanté Ontario;

p) Envoyer des messages anonymes ou se faire passer pour quelqu'un d'autre;

q) Vendre, partager ou redistribuer des produits ou des services de cyberSanté Ontario sans son autorisation écrite;

r) S'adonner à des jeux de hasard sur Internet;

s) Se livrer à toute autre activité pouvant engager la responsabilité civile de cyberSanté Ontario.

6. Sécurité

6.1 Les utilisateurs doivent veiller à la protection des justificatifs d'identité permettant d'obtenir directement ou indirectement l'accès aux produits, aux services ou à l'infrastructure technologique de cyberSanté Ontario.

6.2 Les utilisateurs doivent immédiatement aviser le service de dépannage informatique ou l'administrateur système de l'organisme client s'ils ont des raisons de croire ou s'ils savent que des justificatifs d'identité ont été ou pourraient être violés ou compromis.

6.3 Les organismes client qui ont des raisons de croire ou qui savent que des justificatifs d'identité ont été ou pourraient être violés ou compromis doivent aviser cyberSanté Ontario.

7. Violation de la présente politique

7.1 Les utilisateurs et les organismes clients doivent signaler toute violation de la présente politique dont ils ont connaissance à cyberSanté Ontario. Les utilisateurs doivent passer par le service de dépannage informatique qui assure leur soutien technique, alors que les organismes clients doivent communiquer directement avec cyberSanté Ontario.

7.2 cyberSanté Ontario se réserve le droit de faire enquête sur les cas soupçonnés de violation de la présente politique, et les utilisateurs ainsi que les organismes clients doivent apporter leur collaboration lorsqu'ils sont invités à prêter leur concours à de telles enquêtes.

7.3 cyberSanté Ontario peut, à sa discrétion, suspendre ou révoquer l'accès à ses produits, à ses services ou à son infrastructure technologique lorsqu'un utilisateur viole la présente politique.

7.4 Les organismes clients doivent apporter leur collaboration à cyberSanté Ontario pour la gestion des violations de la présente politique. Cette responsabilité comprend notamment l'aide à la rédaction et à la diffusion de messages concernant les violations ou les incidents.

7.5 La violation de la présente politique peut entraîner des poursuites pénales ou civiles.

7.6 Bien qu'il ne soit pas tenu de surveiller le contenu et n'assume aucune responsabilité à l'égard des renseignements ou du matériel transmis par les utilisateurs des produits, des services, de l'infrastructure technologique ou d'Internet, cyberSanté Ontario se réserve le droit, compte tenu des lois relatives à la protection des renseignements personnels, de faire enquête sur le contenu affiché ou transmis au moyen de son infrastructure technologique et peut bloquer l'accès aux renseignements ou au matériel qui, à son avis, viole la présente politique. Il peut également refuser d'afficher ces renseignements ou ce matériel ou les effacer.

7.7 cyberSanté Ontario peut signaler les violations de la présente politique par un utilisateur à l'organisme client responsable des actions de cet utilisateur.

7.8 cyberSanté Ontario n'assume aucune responsabilité à l'égard de l'application ou de la non-application de la présente politique, et le fait pour cyberSanté Ontario de ne pas appliquer un volet de la présente politique ne constitue pas pour autant une renonciation de sa part au droit de le faire appliquer à quelque moment que ce soit.

7.9 Si une disposition de la présente politique est jugée non valide ou inopérante, elle sera appliquée dans la limite de ce qui est permis, et toutes les autres dispositions demeureront en vigueur.

Pièce C – Politique de sécurité.

1. **Définitions supplémentaires.** En plus des définitions énoncées ailleurs dans la présente convention, les définitions suivantes s'appliquent à la présente annexe :
   (a) « Équipement du client » signifie l'équipement ou les logiciels qui sont en possession ou sous le contrôle du client et que celui-ci utilise conjointement avec le service et qui ne sont pas un équipement lié au service.
   (b) « Réseau du client » signifie tout réseau exploité ou contrôlé par le client, jusqu'au point de démarcation où de tels réseaux sont connectés à l'infrastructure technologique de cyberSanté Ontario.
   (c) « Réseau ONE Network à distance » signifie le réseau privé virtuel à distance.
   (d) « ONE Network » signifie le réseau privé géré qui est exploité par cyberSanté Ontario.

2. **Mesures de protection de cyberSanté Ontario.** cyberSanté Ontario a conçu et mis en œuvre le réseau ONE Network en tant que réseau privé sécurisé qui permet aux professionnels de la santé de communiquer entre eux. Pour obtenir de plus amples renseignements sur les mesures de protection utilisées par cyberSanté Ontario, veuillez prendre contact avec cyberSanté Ontario.

3. **Données du client.** Le client assume la responsabilité des documents qu'il transmet sur le réseau ONE Network et de déterminer si ces documents peuvent être transmis de façon appropriée sur le réseau ONE Network sans cryptage ou autres mesures de protection, compte tenu de la nature et de la sensibilité des documents transmis. Si le client détermine que des mesures de protection sont requises lors de la transmission de tels documents, il se chargera de les mettre en œuvre. De plus, le client assume la responsabilité de vérifier l'exactitude de toute donnée qu'il reçoit par l'entremise du réseau ONE Network.

4. **Équipement.** Le client assume la responsabilité de la sécurité de l'équipement lié au service et de ses propres actifs tangibles, y compris, notamment, l'équipement, les locaux et les services publics du client. Cette obligation inclut le maintien d'un inventaire des actifs du client qui font partie du réseau du client, l'identification de risques possibles et la mise en œuvre de mesures administratives, techniques et physiques pour protéger de tels actifs.

5. **Mesures de protection.** Le client assume la responsabilité de gérer la sécurité de l'équipement du client afin de limiter raisonnablement le risque qu'on y accède et qu'on l'utilise pour attaquer le réseau ONE Network de cyberSanté Ontario ou les systèmes qui y sont reliés. Cette obligation inclut, notamment, l'établissement de politiques de sécurité et la mise en œuvre de contrôles physiques, procéduraux et techniques appropriés afin de prévenir et détecter les atteintes à la sécurité et y répondre.

6. **Aucun changement.** Le client ne doit pas se connecter à l'équipement lié au service, le reconfigurer ou le modifier d'aucune manière sans l'approbation écrite préalable de cyberSanté Ontario.

7. **Infrastructure et environnement.** Le client fournira l'infrastructure et l'environnement nécessaires au fonctionnement sécuritaire de l'équipement lié au service, par exemple installer cet équipement dans un endroit propre, sec, bien ventilé et à température contrôlée, et fournir une alimentation sans coupure appropriée. Tout l'équipement lié au service doit être installé dans une baie ou sur une tablette appropriée et doit être positionné de manière à fournir un espace de travail suffisant dans l'équipement et autour de celui-ci.

8. **Compatibilité.** De temps à autre, cyberSanté Ontario peut fournir au client certaines lignes directrices relatives à l'équipement du client. Le client reconnaît qu'il est possible qu'il ne puisse pas recevoir et utiliser les services, en raison de problèmes de compatibilité, si l'équipement du client ne respecte pas ces lignes directrices.

9. **Sécurité du réseau du client**. Le client assume la responsabilité de la sécurité et du fonctionnement du réseau du client, et il prendra des moyens organisationnels, administratifs, physiques et techniques pour limiter l'accès physique et virtuel à tout terminal informatique ou autre dispositif relié au réseau ONE Network. Le client devra :
   (a) installer et mettre à jour régulièrement des logiciels antivirus et antipourriel raisonnables sur le réseau du client;
   (b) surveiller régulièrement le réseau du client pour détecter toute atteinte à la sécurité;
   (c) mettre en œuvre les mesures de contrôle raisonnablement nécessaires pour prévenir les atteintes à la sécurité relatives au réseau du client et, dans tous les cas, prendre des mesures commercialement raisonnables pour minimiser les répercussions de toute atteinte à la sécurité sur le réseau du client; et
   (d) surveiller régulièrement le réseau du client et les applications utilisées sur celui-ci d'une manière conforme aux bonnes pratiques d'administration de réseau.

10. **Contrôle de l'accès.** Le client aura recours à des moyens organisationnels, administratifs, physiques et techniques pour protéger les identifiants des utilisateurs, les mots de passe, les jetons sécurisés et les autres justificatifs d'authentification assignés au client ou à ses utilisateurs finaux pour leur permettre de se connecter au réseau ONE Network ou à obtenir des services par l'entremise du réseau ONE Network.

11. **Mots de passe.** Si le client détermine qu'un mot de passe ou un autre justificatif d'authentification a été compromis ou a pu l'être, la principale personne-ressource du client (indiquée sur le formulaire du client, au début de la présente convention) signalera l'incident ou la préoccupation au service de dépannage qui fournit le soutien technique au client.

12. **Programme.** Le client établira son propre programme de sécurité qui inclut une approche aux interventions en cas d'incident et un processus de gestion des risques. Au minimum, le client doit déclarer immédiatement à sa principale personne-ressource, et faire en sorte que les utilisateurs finaux en fassent de même, tous les incidents relatifs à la sécurité, réels ou potentiels, qui affectent le réseau ONE Network ou tout autre réseau connecté à celui-ci et dont ils sont mis au courant, et la principale personne-ressource du client doit les signaler au service de dépannage qui fournit le soutien technique au client. Lorsqu'il déclare un tel incident, le client doit fournir tous les renseignements qu'il peut raisonnablement fournir concernant cet incident relatif à la sécurité, ainsi qu'une aide raisonnable pour permettre à cyberSanté Ontario de vérifier et de résoudre l'incident en question.cyberSanté Ontario fera des efforts commercialement raisonnables pour résoudre chaque incident relatif à la sécurité.

13. **Réseaux de tiers.** Le client assume la responsabilité : (i) de mettre en place des mesures de protection (y compris des passerelles de sécurité et des pare-feu) afin d'éviter que tout trafic sur le réseau originaire d'un réseau tiers soit acheminé au réseau ONE Network par l'entremise du réseau du client; et (ii) de maintenir sur le réseau du client des mesures de contrôle appropriées relatives à la configuration et à la sécurité afin de s'assurer raisonnablement qu'aucune personne qui accède au réseau du client par l'entremise d'un réseau tiers puisse utiliser tout dispositif informatique faisant partie du réseau du client pour obtenir un accès non autorisé au réseau ONE Network. Si cyberSanté Ontario, agissant raisonnablement (après avoir fourni au client l'occasion d'améliorer ses mesures de protection pour la sécurité), détermine que le client est incapable de sécuriser le réseau du client décrit dans le présent article 13, le client convient d'abandonner les connexions entre le réseau du client et tout réseau autre que le réseau ONE Network qui sont requises pour sécuriser ainsi le réseau du client.

14. **Pare-feu.** cyberSanté Ontario recommande au client de déployer un pare-feu entre l'équipement de réseau fourni par cyberSanté Ontario et le réseau du client. Le client assume la responsabilité de créer et d'administrer sa propre solution de réseau privé virtuel à distance, de gérer et d'administrer son pare-feu, et de s'assurer que le service de pare-feu effectue la traduction d'adresses de réseau (NAT) et l'inspection dynamique de paquets.

15. **Réseau local d'entreprise**. Le client assume la responsabilité de la gestion de l'espace adresses de son propre réseau local d'entreprise, y compris l'utilisation potentielle de services DHCP et DNS, et de l'acheminement de l'espace adresses de son réseau local d'entreprise.

16. Outils. Le client ne doit pas exécuter d'outils de contournage réseau, d'évaluation des vulnérabilités, de piratage ou de configuration sur l'équipement lié au service ni sur les circuits réseau fournis dans le cadre de la présente convention.

17. **Personnes-ressources du client.** La principale personne-ressource du client assume la responsabilité de la coordination de toutes les questions relatives à l'accès par les utilisateurs finaux (y compris les changements de mots de passe et l'ajout, la modification ou la suppression d'utilisateurs finaux auprès de cyberSanté Ontario) et sera l'unique représentant du client qui sera autorisé à transmettre les demandes associées à cyberSanté Ontario.

18. **Conformité.** À la demande de cyberSanté Ontario, agissant raisonnablement, le client lui fournira une preuve de sa conformité avec une partie ou la totalité de la présente politique de sécurité.