



Epac 3

Proposition d'affaire nouvelle

Cyberrisques, Formule complète

Comment remplir la présente proposition

Vous pouvez remplir le présent document PDF directement à l'écran.

Veuillez répondre en entier à toutes les questions. Au besoin, comme il est indiqué dans les questions ci-dessous, veuillez fournir des renseignements supplémentaires dans un document séparé arborant l'en-tête de votre entreprise et joignez-le à la présente proposition.

Une fois la proposition dûment remplie, un représentant autorisé du proposant doit y inscrire la date et y apposer sa signature.

AVIS

Veuillez prendre note que l'assurance visée par la présente proposition prévoit que les montants des frais et des coûts de défense engagés réduisent le montant de garantie disponible de la police et peuvent l'épuiser complètement. CNA n'assume aucune responsabilité à l'égard des frais ou coûts de défense engagés, des règlements effectués ou des jugements accordés après l'épuisement de ce montant de garantie. Veuillez également prendre note que le montant des frais et coûts de défense engagés sera soumis à la rétention applicable. Le présent avis est assujéti aux dispositions du Code civil du Québec qui s'appliquent à la police établie.

Le fait de fournir des renseignements au sujet d'une réclamation ou d'une réclamation éventuelle en réponse à une question formulée dans la présente proposition n'implique pas que cette réclamation est couverte ou le sera. Le défaut du proposant de déclarer à sa compagnie d'assurance actuelle une réclamation présentée contre lui pendant la présente période d'assurance ou de déclarer un acte, une omission ou une circonstance connus de lui et susceptible de donner lieu à une réclamation ou des dommages subis par l'assuré, avant l'expiration de la police actuelle, peut entraîner une absence de couverture d'assurance.

À noter que la présentation d'une proposition dûment remplie et signée n'oblige pas un proposant à souscrire l'assurance ni la compagnie d'assurance à accorder l'assurance.

I. RENSEIGNEMENTS SUR LE PROPOSANT

Proposant à désigner au point 1 des Conditions particulières (l'« assuré désigné ») : _____

Adresse : _____

Ville : _____ Province : _____ Code postal : _____

Site(s) Interne : _____ Numéro de téléphone : _____

a. Date de constitution du proposant : _____

b. Structure du capital social :

☐ Société fermée ☐ Société ouverte ☐ Organisme sans but lucratif ☐ Organisme gouvernemental

c. Type d'entreprise :

☐ Société par actions ☐ Société de personnes ☐ Coentreprise ☐ SARL

d. Nombre d'employés : _____

e. Demandez-vous une assurance à l'égard d'un autre « assuré désigné » ou de filiales, de sociétés affiliées ou d'autres entités connexes ? ☐ Oui ☐ Non

Si vous avez répondu « Oui » à la question ci-dessus, veuillez fournir des précisions _____

f. Le proposant est-il entièrement ou partiellement détenu ou contrôlé par une autre entité ? ☐ Oui ☐ Non

Si vous avez répondu « Oui » à la question ci-dessus, veuillez fournir le nom, la date de constitution, le lieu et le degré de contrôle de chacune de ces entités :

g. Le proposant, exclusivement ou non exclusivement, détient-il, contrôle-t-il, gère-t-il ou exploite-t-il une autre entité non énumérée dans la présente proposition ? ☐ Oui ☐ Non

Si vous avez répondu « Oui » à la question ci-dessus, veuillez fournir des précisions complètes :

h. Région ou territoire des activités :

☐ Local ☐ Régional ☐ National ☐ International

i. Quelle est la nature des activités du proposant ? _____

II. GARANTIES DEMANDÉES

Garantie	Montant de garantie	Rétention	Date de rétroactivité
Cyberrisques	_____ \$	_____ \$	_____

III. RENSEIGNEMENTS SUR L'ASSURANCE ARRIVANT À L'ÉCHÉANCE

1. Veuillez fournir les renseignements demandés ci-dessous à l'égard des garanties aux termes desquelles vous êtes actuellement assuré :

Garantie	Montant de garantie	Rétention	Date de rétroactivité	Prime	Assureur	Date d'expiration
Cyberrisques	_____ \$	_____ \$	_____	_____ \$	_____	_____

2. L'assureur de l'une des garanties énumérées ci-dessus vous a-t-il informé de son intention de ne pas renouveler les conditions de la garantie ?

☐ Oui ☐ Non

IV. RENSEIGNEMENTS GÉNÉRAUX

Indiquez si, au cours des 18 derniers mois ou des 12 prochains mois, le proposant ou une filiale ont fait l'objet ou prévoient de faire l'objet de l'une des situations suivantes :

- a. Fusion, consolidation, acquisition ou dessaisissement ☐ Oui ☐ Non
- b. Changement important sur le plan de la nature ou de l'ampleur des activités ☐ Oui ☐ Non
- c. Dépôt de bilan ou réorganisation ☐ Oui ☐ Non

Si vous avez répondu « Oui » à l'une des questions ci-dessus, veuillez fournir des précisions complètes (si l'espace est insuffisant, fournir l'information manquante dans un document séparé) :

V. RENSEIGNEMENTS FINANCIERS

1. Veuillez indiquer le chiffre d'affaires brut du proposant.

Exercice précédent	Exercice courant	Montant prévu
_____ \$	_____ \$	_____ \$

2. Veuillez indiquer le pourcentage du chiffre d'affaires du proposant réalisé au Canada par rapport au pourcentage réalisé à l'étranger :

Canada : _____ % États-Unis : _____ % Étranger : _____ %

VI. RENSEIGNEMENTS SUR LES RÉCLAMATIONS

1. Un avis de réclamation, de réclamation éventuelle, de dommages subis par l'assuré (y compris, mais sans s'y limiter, une atteinte à la sécurité des données, une atteinte à la sécurité, une menace d'extorsion ou demande de sommes relatives à une extorsion, ou la publication, la perte ou la divulgation de renseignements permettant d'identifier une personne placée sous la garde ou la responsabilité du proposant ou confiés à ses soins, ou l'accès non autorisé à ceux-ci), ou d'éventuels dommages subis par l'assuré a-t-il été transmis à un assureur à l'égard d'une garantie demandée par le proposant ?

☐ Oui ☐ Non

2. Au cours des 3 dernières années, est-ce que le proposant, une filiale ou une personne associée à l'une des entités pour lesquelles l'assurance est demandée (« assurés proposés ») a fait l'objet d'une réclamation, d'une demande écrite, d'un avis, d'une procédure, d'un litige ou d'une enquête, ou y a participé, lesquels sont fondés sur des allégations :
- a. De violation d'une loi ou d'un règlement sur la protection des renseignements personnels ou la sécurité des données ? ☐ Oui ☐ Non
 - b. D'atteinte à la vie privée, de vol d'identité, d'attaque par déni de service, d'infection par virus informatique, de vol de renseignements, de dommages causés à des réseaux de tiers ou d'incapacité des utilisateurs autorisés du proposant ou d'une filiale d'accéder au réseau de ces derniers ? ☐ Oui ☐ Non
 - c. De perte d'argent, de valeurs mobilières ou de biens découlant d'un acte de piratage psychologique, d'une fraude ou d'un autre acte criminel ? ☐ Oui ☐ Non
3. Au cours des 3 dernières années, un assuré proposé a-t-il fait l'objet d'une recherche, d'une enquête ou d'une mesure disciplinaire par un organisme ou une association réglementaires ou administratifs ? ☐ Oui ☐ Non
4. Au cours des 3 dernières années, un assuré proposé a-t-il appris l'existence d'éventuels dommages subis par l'assuré (y compris, sans s'y limiter, une atteinte à la sécurité des données, une atteinte à la sécurité, une menace d'extorsion ou demande de sommes relatives à une extorsion, ou la publication, la perte ou la divulgation de renseignements permettant d'identifier une personne placés sous la garde ou la responsabilité du proposant ou confiés à ses soins, ou l'accès non autorisé à ceux-ci), qu'ils aient ou non été déclarés à un assureur antérieur ? ☐ Oui ☐ Non

Si vous avez répondu « Oui » à l'une des questions des paragraphes 1 à 4 ci-dessus, veuillez fournir des précisions, y compris la date, le type de réclamation ou de dommages subis par l'assuré, les allégations, l'état actuel, les frais de défense engagés, ainsi que les montants des jugements accordés ou des règlements effectués (si l'espace est insuffisant, veuillez fournir les renseignements manquants dans un document séparé) :

VII. PARTIE D'ASSURANCE DES CYBERRISQUES

A. Renseignements sensibles

1. Veuillez indiquer les renseignements sensibles sur les employés ou les clients qui sont en possession du proposant :

Type de renseignement	Nombre estimat de dossiers	Ces dossiers sont-ils chiffrés au repos ?	Ces dossiers sont-ils chiffrés en mouvement ?
Numéros d'assurance sociale		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Numéros de permis de conduire		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Numéros de compte financier		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Numéros de carte de crédit		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Renseignements personnels sur la santé		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Données biométriques		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Secrets commerciaux de tiers		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Propriété intellectuelle de tiers		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Renseignements financiers d'une entreprise tierce		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet
Total		☐ Oui ☐ Non	☐ Oui ☐ Non ☐ Sans objet

2. Les données mentionnées à la question 1 ci-dessus font-elles l'objet d'une ségrégation ? ☐ Oui ☐ Non

vous avez répondu « Oui » à la question ci-dessus, quel est le plus grand nombre de dossiers conservés au même endroit ?

3. Certains des renseignements mentionnés à la question 1 ci-dessus sont-ils stockés sur des appareils mobiles (p. ex., ordinateurs portables, tablettes, téléphones cellulaires) ? ☐ Oui ☐ Non

Si vous avez répondu « Oui » à la question ci-dessus, les renseignements sont-ils chiffrés au repos et en mouvement ? ☐ Oui ☐ Non

4. Certains des renseignements mentionnés à la question 1 ci-dessus proviennent-ils de personnes qui ne sont pas des résidentes du Canada ou d'entreprises qui ne sont pas domiciliées au Canada ? ☐ Oui ☐ Non ☐ S. O.

B. Politiques sur la sécurité de l'information et la protection de la vie privée

1. Veuillez indiquer si le proposant :	Oui	Non
a. Compte une personne responsable de la protection de la vie privée et de la sécurité de l'information.	☐	☐
b. Compte une personne responsable de surveiller les changements apportés aux lois et aux règlements sur la protection de la vie privée et la sécurité de l'information.	☐	☐
c. A mis en place des politiques, des normes ou des procédures écrites officielles en matière de sécurité de l'information et de protection de la vie privée aux fins de l'administration de la sécurité de l'information dans l'ensemble de votre organisation.	☐	☐
d. A mis en place une politique écrite de conservation des dossiers qui prévoit l'élimination ou la suppression sécurisée des dossiers papier ou électroniques, ainsi que des renseignements biométriques et autres lorsqu'ils ne sont plus nécessaires.	☐	☐
e. Conserve les données uniquement lorsqu'il est nécessaire de le faire pour la prestation de services.	☐	☐
f. A fait examiner les politiques de sécurité de l'information et de protection de la vie privée par un avocat externe spécialisé en droit de la vie privée.	☐	☐
g. A mis en place un programme officiel de sensibilisation à la sécurité et de formation connexe visant à soutenir les normes et politiques, nouvelles et existantes, et à les communiquer aux employés.	☐	☐
h. Exige que toutes les personnes de l'organisation suivent régulièrement une formation de sensibilisation à la sécurité pour lutter contre la fraude portant notamment sur la détection des manœuvres d'ingénierie sociale, d'hameçonnage ou d'autres arnaques similaires.	☐	☐
i. A mis en place un processus officiel et exhaustif d'intégration des employés (y compris la vérification des antécédents, le dépistage de drogues, la recherche d'un éventuel casier judiciaire, la vérification des antécédents en matière de crédit, etc.).	☐	☐

2. Le proposant se conforme-t-il :	Oui	Non	S. O.
a. À la LPRPDE ou aux lois ou règlements provinciaux en matière de protection des renseignements personnels ou des renseignements personnels sur la santé sensiblement similaires ?	☐	☐	☐
b. Au règlement général sur la protection des données de l'Union européenne ?	☐	☐	☐

- | | | | |
|---|-----------------------|-----------------------|-----------------------|
| c. À la loi des États-Unis intitulée <i>Health Insurance Portability and Accountability Act</i> ? | ☐ | ☐ | ☐ |
| d. À la loi californienne intitulée <i>California Consumer Privacy Act</i> ? | ☐ | ☐ | ☐ |
| e. Aux lois ou règlements du fédéral, d'une province, d'un territoire ou d'un État relatifs aux renseignements biométriques ? | ☐ | ☐ | ☐ |

C. Mécanismes de contrôle de la sécurité d'un réseau

1. Le proposant :	Oui	Non
a. Utilise-t-il des systèmes d'exploitation qui ne sont pas pris en charge (p. ex., Windows XP ou Server 2003) ?	☐	☐
b. Évalue-t-il les applications et l'infrastructure afin de repérer les vulnérabilités courantes en matière de sécurité (p. ex., en utilisant les outils OWASP top 10 ou SANS 20) ?	☐	☐
c. Remplace-t-il les paramètres d'usine par défaut (y compris les noms d'utilisateur et les mots de passe) pour s'assurer que vos systèmes de sécurité de l'information sont configurés de manière sécurisée ?	☐	☐
d. A-t-il instauré un mécanisme de ségrégation des tâches pour ce qui est des environnements de développement, de test et de production ?	☐	☐
e. Vérifie-t-il la disponibilité de correctifs de sécurité pour vos systèmes au moins une fois par semaine, qu'il installe, le cas échéant, dans un délai de 30 jours ?	☐	☐
Si vous avez répondu « Non », veuillez décrire brièvement votre processus d'application de correctifs :	☐	☐
2. À quelle fréquence le proposant soumet-il son réseau et ses applications à des tests de pénétration réguliers effectués par des tiers ?		
3. Des mesures correctives ont-elles été apportées à l'égard de toutes les failles de niveau moyen, élevé ou critique décelées lors du test le plus récent ?	☐ Oui	☐ Non
4. À quelle fréquence le proposant procède-t-il à des évaluations officielles des risques ?		
5. Le proposant sauvegarde-t-il régulièrement les données, les applications et les configurations de système ?	☐ Oui	☐ Non
Si vous avez répondu « Oui » à la question ci-dessus, les sauvegardes sont-elles :		
a. Soumises régulièrement à des tests visant à vérifier leur récupérabilité ?	☐ Oui	☐ Non
b. Stockées hors site et hors ligne ?	☐ Oui	☐ Non
c. Chiffrées au repos ?	☐ Oui	☐ Non

6. Le proposant s'est-il doté :	Oui	Non
a. D'un logiciel antivirus à jour ?	☐	☐
b. D'un mécanisme d'authentification à facteurs multiples pour la connexion à distance à son réseau ?	☐	☐
c. D'un mécanisme d'authentification à facteurs multiples pour l'accès des utilisateurs privilégiés ?	☐	☐
d. D'un réseau privé virtuel (VPN), d'un VPN SSL ou d'une technologie équivalente ?	☐	☐
e. D'un système de gestion des informations et des événements de sécurité ?	☐	☐
f. D'une technologie de prévention de fuite de données ou de tout autre programme ou toute autre technologie similaire ?	☐	☐
g. Du protocole d'authentification et de chiffrement Wi-Fi Protected Access 2 ou d'un protocole plus robuste pour son réseau sans fil ?	☐	☐
h. De pratiques et de mécanismes de contrôle en matière de mots de passe (p. ex., longueur minimale du mot de passe, caractères spéciaux ou lettres majuscules) ?	☐	☐

7. Le proposant :	Oui	Non
a. Contrôle-t-il l'accès à votre système pour s'assurer que les utilisateurs n'ont accès qu'aux environnements dont ils ont besoin pour accomplir leur travail ?	☐	☐
b. Vérifie-t-il l'accès des utilisateurs pour s'assurer que le niveau d'autorisation accordé aux employés n'excède pas celui exigé par leurs responsabilités professionnelles ?	☐	☐
Si vous avez répondu « Oui », à quelle fréquence cette vérification a-t-elle lieu ? _____		
c. Supprime-t-il rapidement l'accès aux systèmes lorsqu'une personne quitte l'organisation ou lorsque l'accès n'est plus nécessaire à des fins professionnelles ?	☐	☐
Dans quel délai cette mesure est-elle prise ? _____		
d. Restreint-il l'accès physique à toutes les situations à votre propre personnel ainsi qu'aux sous-traitants, agents ou visiteurs autorisés uniquement ?	☐	☐

8. Le proposant exige-t-il le respect des mesures suivantes pour contrôler l'accès aux centres de données et aux armoires réseau :	Oui	Non
a. Badge d'accès	☐	☐
b. Biométrie	☐	☐
c. Verrouillage automatique	☐	☐
d. Signal d'alarme avec minuterie pour les portes ouvertes	☐	☐

D. Plans d'intervention en cas d'incident, de continuité des activités ou de reprise après catastrophe

1. Le proposant a-t-il mis en place l'un des plans officiels suivants :

- a. Plan d'intervention en cas d'incident ☐ Oui ☐ Non
- b. Plan de continuité des activités ☐ Oui ☐ Non
- c. Plan de reprise après catastrophe ☐ Oui ☐ Non

Si vous avez répondu « Oui » à l'une des questions ci-dessus, à quelle fréquence ces plans sont-ils mis à l'épreuve ?

2. Si le réseau du proposant faisait l'objet d'une perturbation, combien de temps faudrait-il pour le rétablir complètement ?

- ☐ De 1 à 4 heures ☐ De 4 à 8 heures ☐ De 8 à 12 heures
- ☐ De 12 à 24 heures ☐ De 24 à 48 heures ☐ 48 heures et plus

E. Fournisseurs tiers et fournisseurs de services

1. Lorsque le proposant confie des renseignements sensibles à des tiers :	Oui	Non
a. Exige-t-il par contrat que tous ces tiers protègent ces renseignements au moyen de mesures de protection au moins équivalentes aux siennes ?	☐	☐
b. Fait-il preuve de diligence raisonnable à l'égard de chacun de ces tiers pour s'assurer que leurs mesures de protection des renseignements sensibles respectent les normes du proposant (p. ex., effectuer des vérifications de sécurité et de confidentialité ou examiner les conclusions de vérificateurs indépendants en matière de sécurité et de confidentialité) ?	☐	☐
c. Effectue-t-il des vérifications de tous ces tiers au moins une fois par année pour s'assurer qu'ils continuent de respecter les normes du proposant en matière de protection des renseignements sensibles ?	☐	☐
d. Les oblige-t-il par contrat écrit à défendre et à indemniser le proposant s'ils contribuent à une atteinte à la confidentialité, à la sécurité ou à la vie privée ?	☐	☐
e. Oblige-t-il tous ces tiers à disposer de liquidités suffisantes ou à souscrire une assurance de responsabilité professionnelle d'un montant suffisant pour couvrir leur responsabilité découlant d'une atteinte à la vie privée ou à la confidentialité ?	☐	☐
f. Exige-t-il des rapports SOC 2 ?	☐	☐

2. Fournisseurs de services réseautiques et technologiques actuels (s'il y a lieu)

Fournisseur(s) de services Internet

Fournisseur(s) de services infonuagiques

Hébergement de site Internet

Services de collocation

Traitement de carte de crédit

Services de gestion de la sécurité

Autre(s)

3. Quel pourcentage du chiffre d'affaires du proposant dépend directement de sites Internet publics ? _____ %
4. Quelle est la durée minimale d'interruption du système à partir de laquelle le proposant s'attend à une incidence quantifiable sur son chiffre d'affaires ? _____

F. Renseignements personnels sur la santé

1. Le proposant traite-t-il, transmet-il, stocke-t-il ou utilise-t-il des renseignements personnels sur la santé ? ☐ Oui ☐ Non

2. Si vous avez répondu «Oui» à la question ci-dessus	Oui	Non
a. Une analyse des risques est-elle effectuée pour déterminer où les renseignements personnels sur la santé sont utilisés et stockés afin de repérer les lacunes et les menaces éventuelles pour lesdits renseignements personnels sur la santé ?	☐	☐
b. L'accès aux données ou renseignements personnels sur la santé est-il limité aux personnes qui en ont besoin ?	☐	☐
c. Un plan d'intervention en cas d'incident spécifique aux renseignements personnels sur la santé a-t-il été mis en place ?	☐	☐
d. Les utilisateurs reçoivent-ils une formation sur la sécurité des renseignements personnels sur la santé ?	☐	☐
e. Les mesures de contrôle de la sécurité des renseignements et de la protection de la vie privée mentionnées ci-dessus ont-elles été mises en place à l'égard des renseignements personnels sur la santé qui sont en possession du proposant ou sous sa responsabilité ?	☐	☐

G. Renseignements liés aux cartes de paiement

1. Le proposant accepte-t-il les paiements par carte de crédit ou de débit ? ☐ Oui ☐ Non

Si vous avez répondu «Non» à la question ci-dessus, veuillez passer à la section H, Cybercriminalité.

2. Le proposant a-t-il confirmé sa conformité aux normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS) ? ☐ Oui ☐ Non
- a. Dans l'affirmative, à quelle version des normes PCI DSS le proposant se conforme-t-il ? _____
- b. Combien d'opérations le proposant réalise-t-il annuellement ? _____
- c. Pour quel pourcentage d'opérations réalisées par le proposant la technologie Europay MasterCard Visa (EMV avec puce et NIP) ou un système de segmentation en unités similaire est-il utilisé ? _____ %

3. Si vous avez répondu «Oui» à la question ci-dessus :	Oui	Non
a. La segmentation est-elle mise en œuvre pour isoler les renseignements régis par les normes PCI DSS du reste du réseau de l'entreprise ?	☐	☐
b. La segmentation en unités est-elle réalisée pour supprimer le numéro de carte de crédit de l'opération ?	☐	☐
c. Une politique et une procédure visant à appliquer des correctifs sur les appareils des points de vente ont-elles été mises en place ?	☐	☐
d. Des restrictions de connectivité ont-elles été appliquées pour empêcher l'accès à Internet ?	☐	☐

- | | | |
|--|-----------------------|-----------------------|
| e. La sécurité des appareils aux points de vente a-t-elle été renforcée par l'établissement d'une liste d'autorisation d'applications ? | ☐ | ☐ |
| f. Le chiffrement de bout en bout est-il utilisé dès que les renseignements liés à la carte de crédit sont lus dans l'appareil au point de vente ? | ☐ | ☐ |

4. Veuillez indiquer si les renseignements ci-après sont placés sous la garde ou la supervision du proposant ou confiés à ses soins :	Oui	Non
a. Données liées à la carte de crédit pendant la durée de l'opération	☐	☐
b. Données liées à la carte de crédit stockées pour utilisation future (tous les chiffres sont masqués, sauf les quatre derniers)	☐	☐
c. Données liées à la carte de crédit stockées pour utilisation future (numéros de carte non masqués, y compris les données de la piste 2)	☐	☐

H. Cybercriminalité

(à remplir uniquement si le proposant demande la garantie Cybercriminalité)

1. Le proposant :	Oui	Non
a. A-t-il mis en place des procédures visant à vérifier que les stocks, les fournitures, les biens ou les services reçus correspondent à ceux qui ont été facturés avant de payer un fournisseur ?	☐	☐
b. A-t-il adopté une politique écrite sur les virements électroniques de fonds ?	☐	☐
c. Accepte-t-il les instructions de virement de fonds ou demandes de modification des renseignements sur les comptes provenant de sources internes (p. ex., employés) ou externes (p. ex., clients, fournisseurs) par téléphone, télécopieur, courriel ou tout autre mode de communication électronique ?	☐	☐
Si vous avez répondu « Oui », avant de donner suite aux instructions, le proposant les valide-t-il en utilisant une méthode différente de celle qui a servi au contact initial ?		
☐ Oui ☐ Non		
d. Accorde-t-il à certains employés uniquement l'autorisation d'effectuer des virements électroniques ?	☐	☐
e. Limite-t-il l'accès au portail d'opérations bancaires en ligne utilisé pour effectuer des virements électroniques à des utilisateurs déterminés à partir de terminaux précis ?	☐	☐
f. Exige-t-il que les paiements ou virements de fonds d'un montant donné fassent l'objet d'une autorisation double ?	☐	☐
Si vous avez répondu « Oui », quel est ce montant ? _____ \$		
g. A-t-il mis en place des politiques et des procédures différentes à l'égard des virements électroniques de fonds internationaux ?	☐	☐
Si oui, veuillez fournir des explications sur une feuille séparée jointe à la présente proposition.		

- Quel est le nombre moyen de virements de fonds par mois ? _____
- Quel est le montant moyen par virement de fonds ? _____ \$
- Quel est le montant le plus élevé qui peut être viré ? _____ \$

DÉCLARATIONS DU PROPOSANT

(à remplir par le proposant)

Les déclarations du proposant s'appliquent à toutes les garanties qui ont été demandées dans le cadre de la présente proposition.

1. Déclaration particulière applicable aux garanties suivantes uniquement (si elles doivent faire partie de la police) :

Dans le cas de la garantie désignée par un crochet ci-dessous, le proposant détient une assurance soit auprès de CNA soit auprès d'un autre assureur :

Garanties	L'assurance est en place depuis :
☐ Cyberrisques	_____

Le proposant demande la continuité de cette garantie et la déclaration du proposant ci-dessous ne s'applique pas à cette garantie.

Si aucune case n'est cochée ci-dessus, cette déclaration du proposant s'applique à cette garantie si celle-ci est demandée dans la proposition, sous réserve de ce qui suit :

Déclaration du proposant – Aucune des personnes à assurer aux termes de la partie d'assurance Cyberrisques n'est responsable ou n'est au courant d'un acte préjudiciable, d'un fait, d'une circonstance ou d'une situation susceptibles de donner lieu à une réclamation future ou à des dommages subis par l'assuré, sauf ce qui suit :

- ☐ Oui, il existe des exceptions à cette déclaration (veuillez fournir des précisions).
- ☐ Non, il n'existe aucune exception à cette déclaration.

Si un acte préjudiciable, un fait, une circonstance ou une situation est susceptible de donner lieu à une réclamation future ou à des dommages subis par l'assuré, que cet acte préjudiciable, ce fait, cette circonstance ou cette situation soient déclarés ci-dessus ou non, le proposant reconnaît et convient, à moins que la police d'assurance envisagée ne prévoie expressément autrement, que tout sinistre, toute réclamation, toute action ou tous dommages subis par l'assuré liés, attribuables ou consécutifs à cet acte préjudiciable, à ce fait, à cette circonstance ou à cette situation seront exclus de l'assurance conformément aux dispositions de la proposition d'assurance.

2. Déclarations applicables à toutes les garanties devant faire partie de la police :

Le proposant déclare, après enquête menée avec diligence, que les renseignements contenus dans la présente proposition et dans toute proposition supplémentaire ou tout formulaire devant accompagner les présentes sont vrais, exacts et complets et qu'aucun fait essentiel n'a fait l'objet d'une réticence ou d'une fausse déclaration. Le proposant reconnaît une obligation continue de déclarer dès que possible à la compagnie CNA (la « Compagnie »), à qui il soumet la présente proposition, tout changement important ayant lieu après la signature de la proposition et avant l'établissement de la police. Le proposant reconnaît par ailleurs que la Compagnie aura le droit de retirer toute soumission, autorisation ou entente en suspens ou de la modifier en fonction de ces changements.

De plus, le proposant comprend et reconnaît que :

- le fait de remplir la présente proposition et toute proposition ou tout formulaire supplémentaire n'oblige pas la Compagnie à émettre une police;
- si une police est émise, la Compagnie s'est fondée sur les déclarations faites dans la présente proposition et dans toute proposition supplémentaire ainsi que sur d'autres déclarations faites à la Compagnie conjointement avec la présente proposition;
- toutes les propositions supplémentaires, tous les énoncés et tout autre matériel fournis à la Compagnie conjointement avec la présente proposition sont incorporés par renvoi à la présente proposition et en font partie intégrante;
- la présente proposition constituera la base du contrat et sera incorporée par renvoi à cette police et en fera partie intégrante;
- si une police est émise, le paiement des sinistres, des frais de défense et des dépenses aura pour effet de réduire le montant de garantie prévu par la police et pourra même l'épuiser complètement. En ce cas, la Compagnie ne prendra pas en charge la partie des sinistres, des frais de défense et des dépenses qui excède le montant de garantie de la police;

- f. si une police est émise, les frais de défense et les dépenses engagés seront assujettis au montant de la franchise ou de la rétention prévue par la police;
- g. le défaut du proposant de déclarer à sa compagnie d'assurance actuelle :
 - i. une réclamation présentée contre lui ou des dommages subis par l'assuré découverts pendant la présente période d'assurance;
 - ii. un acte, une omission ou une circonstance connus de lui et susceptibles de donner lieu à une réclamation ou à des dommages subis par l'assuré, avant l'expiration de la police actuelle, peut entraîner une absence de couverture.

AVIS DE FRAUDE

Toute personne qui, sciemment et dans l'intention de frauder une compagnie d'assurance ou une autre personne, présente une proposition d'assurance renfermant des renseignements qui sont faux ou incomplets, ou qui, dans le but de tromper, dissimule des renseignements concernant des faits essentiels à l'appréciation des risques, commet une fraude d'assurance, qui est un crime passible d'amendes et de pénalités civiles et criminelles.

Le proposant, par l'entremise du représentant autorisé soussigné, reconnaît par les présentes que les déclarations et réponses susmentionnées sont exactes et complètes. Le proposant comprend par ailleurs qu'une déclaration inexacte ou incomplète peut donner lieu à une exclusion ou au refus de l'assurance. De plus, le proposant autorise les sociétés d'assurance CNA à communiquer les renseignements figurant dans la présente proposition ainsi que l'information de souscription connexe.

PROPOSANT

Par : _____
Signature et titre de fonction* Nonm du représentant autorisé en caractères d'imprimerie

Date : _____

*** La présente proposition doit être signée par le chef de la direction, le chef des finances, le chef de l'exploitation, l'avocat général ou le gestionnaire du risque du proposant en sa qualité de représentant autorisé des personnes et entités à assurer. Veuillez imprimer et signer la présente proposition.**

Remarque : Aux fins de la Loi sur les sociétés d'assurances (Canada), le présent document a été rédigé dans le cadre des activités de souscription d'assurance de la Compagnie d'assurance Continental Casualty au Canada.