PROPOSITION SUPPLEMENTAIRE POUR UNE ASSURANCE CONTRE LA FRAUDE INFORMATIQUE

PRIÈRE DE RÉPONDRE À TOUTES LES QUESTIONS, SANS AUCUN BLANC, AU BESOIN, UTILISER «S/O» (SANS OBJET)

Ce formulaire de proposition est pour une police d'assurance ayant trait à des réclamations faites et rapportées à l'Assureur au cours de la période d'assurance.

Preneur **Pourcentage détenu**
%

(Énumérez ceux qui font l'objet de cette Proposition y compris les régimes d'avantages sociaux. S.V.P. éviter d'employer des termes généraux tel que «toutes les filiales, ou entreprises administrées ou contrôlées», etc. Au besoin, priere d'utiliser un feuille distincte.)

Adresse principale:
numéro rue

ville province code postal

Adresse Internet:

Prise d'effet: à minuit une minute, heure normale le

OPTIONS DES MONTANTS ET FRANCHISES DEMANDÉS

(i)	Limite(s) de la garantie	(a)	$	(b)	$
(ii)	Franchise(s)	(a)	$	(b)	$

1. **GARANTIES FACULTATIVES**

(a)	Piratage informatique	Oui ☐ Non ☐
(b)	Contamination par virus	Oui ☐ Non ☐
(c)	Communications électroniques frauduleuses	Oui ☐ Non ☐
(d)	Télécommunications falsifiées	Oui ☐ Non ☐
(e)	Transferts à commande vocale	Oui ☐ Non ☐
(f)	Fraude téléphonique	Oui ☐ Non ☐

2. **CONTRÔLES GÉNÉRAUX ADMINISTRATIFS**

(a)	Votre protocole informatique, a-t-il été formulé par un service centralisé de la technologie informatique?	Oui ☐ Non ☐
(b)	Votre programme de protection anti-virus fait-il objet d'une gestion centralisée?	Oui ☐ Non ☐
(c)	A-t-on établi des normes relatives au maintien des fonctions critiques de votre réseau?	Oui ☐ Non ☐
(d)	Est-ce que vos normes de sécurités informatique sont mise en applications universellement et en toute légalité à travers votre société?	Oui ☐ Non ☐
(e)	Au sein de vos employés, vos sous-traitants ou vos associés, saura-t-on reconnaître une violations de la sécurités informatique?	Oui ☐ Non ☐
(f)	Sont-ils au courant de protocole à suivre advenant une faille en cours dans le système de sécurité?	Oui ☐ Non ☐

3. **PROTECTION ANTI-VIRUS**

(a) Est-ce tous vos ordinateurs et systèmes de réseautage sont dotés de protections anti-virus? Oui ☐ Non ☐

(b) Vos protections anti-virus, sont-ils activées lors du démarrage des systèmes et programmés pour faire un balayage continuel lors de l'usage du système? Oui ☐ Non ☐

(c) La mise à jour et la dissémination des mises à jour de vos protections anti-virus se fait à quelle fréquence?
☐ au jour; ☐ à la semaine; ☐ aux deux semanines; ☐ au mois (ou plus)

4. **CONTRÔLES D'ACCÈS AUX RESEAUX**

(a) De quelle façon contrôlez-vous l'accès a votre reseau?
☐ empreintes digitales; ☐ balayage de retinæ; ☐ mots de passe; ☐ autre (prière d'élaborer)

(b) Pour tout mot de passe, exigez-vous un minimum de huit (8) caratères alpha numérique en minuscule et en majuscule et caractères spéciaux? Oui ☐ Non ☐

(c) Les mot de passe de tous les usagers, sont-ils chiffrés? Oui ☐ Non ☐

(d) À quelle fréquence doit-on obligatoirement modifier son mot de passe?
☐ au 30 jours; ☐ au 60 jours; ☐ au 90 jours (ou plus)

5. **LE DROITS D'ACCÈS**

(a) À l'intérieur de votre société est-ce que tous les postes font l'objet d'une analyse afin d'établir les droits d'accès et lignes d'autorité pour vos systèmes informatiques et réseautiques? Oui ☐ Non ☐

(b) Est-ce que le service des technologies de l'informatique est promptement avisé lors du départ des employés afin de restreindre ou de prévenir immédiatement l'accès aux ordinateurs et aux réseaux? Oui ☐ Non ☐

6. **SÉCURITÉ LAN/WAN**

(a) Est-ce que les identités des usagers de vos réseaux sont authentifiées par moyen d'identifications d'suager et mots de passe distincts? Oui ☐ Non ☐

(b) Permettez-vous aux usagers d'avoir recours à des modems a composition automatique à partir des stations de travail reliées simultanément à un réseau LAN (ou un autre réseau)? Oui ☐ Non ☐

(c) Est-ce que toutes les communications externes (y comprise les connections aux réseaux internes) sont acheminées à travers un coupe feu? Oui ☐ Non ☐

7. **LA SÉCURITÉ INTERNET**

(a) Nombre d'employés ayant accès à l'internet?

(b) Est-vous doté d'un système d'auto-vérifications sur le Web? Oui ☐ Non ☐

(c) Avez-vous établi des normes relatives l'usage d l'Internet de du courriel et dans l'affirmative, ces normes sont-elles appliquées avec rigueur? Oui ☐ Non ☐

(d) Est-ce que votre environnement Internet est protège avec au moins deux (2) coupe-feu? Oui ☐ Non ☐

(e) Si non, combien de coupe feu protège votre environnement Internet?

(f) Y a-t-il système de détection d'intrusion («IDS») relié à votre coupe-feu? Oui ☐ Non ☐

(g) Est-ce que les transactions sur votre réseau longue distance ainsi que vos transactions confidentielles sur Internet sont cryptées avec un minimum de 64 bit? Oui ☐ Non ☐

(h) Utlisez-vous une technologie sans-fil pour accéder à l'Internet? Oui ☐ Non ☐

Dan l'affirmative, quelles mesures de sécurité additionnelle avez-vous instaurées?

(i) Permettez-vous l'accès à distance à votre système? Oui ☐ Non ☐
Dans l'affirmative:
(i) Nombre d'employés avec accès à distance?
(ii) Nombre de clients qui utilise le service en ligne?
(iii) Est-ce que l'accès à distance se limite aux réseaux privés virtuels (VPN)? Oui ☐ Non ☐
(iv) L'accès à distance est permis en utilisant:
☐ des équipements domestiques? ☐ des équipements de la société?

(j) A combien s'élèvent les recette provenant des activités en ligne? $ (CDN)

(k) Quel activités / produits font l'objet des transactions en ligne?

8. **SYSTÈMES DE DÉTECTION DES INTRUSIONS**

(a) Est-ce votre réseau est muni d'un système de détection des intrusions? Oui ☐ Non ☐

Dan l'affirmative, est-ce que tous les systèmes sont dotés d'un registre d'incidents afin de permettre une analyse des attaques? Oui ☐ Non ☐

(b) Quel serait de délai entre la confirmation d'une instusion et le blocage de celle-ci?
☐ moins de quinze minutes ☐ 15 – 30 minutes ☐ 30 – 60 minutes ☐ plus de 60 minutes

9. **PROCEDURES DE SAUVEGARDE**

(a) Est-ce que tous les usagers doivent procéder à une fermeture de session à la fin de la journée ou lorsqu'ils doivent quiter leur station de travail? Oui ☐ Non ☐

(b) Vos sous traitants ont-ils accès à votre réseau après le départ journalier de vos employés? Oui ☐ Non ☐

(c) A quelle fréquence procéde-t-on a la sauvegarde des données critiques?
☐ au jour le jour; ☐ à la semaine; ☐ aux deux semaines; ☐ au mois (ou plus)

10. **CONTRÔLE DES COMMUNICATIONS**

(a) Votre système, est-il muni d'un système de balayage afin de déceler des courriels suspects? Oui ☐ Non ☐

Décrivez le protocoles établi pour accéder aux pièces jointes des courriels:

(b) Un fois chiffrées et authentifiées, utilisez-vous une technologie sans fil de courte ou de longue portée pour les transferts de données sensibles de la corporation? Oui ☐ Non ☐

(c) L'utilisations des sercices de messageries instantanées, est-elle strictement défendue? Oui ☐ Non ☐

11. **TRANSFERTS FRAUDLULEUX DE FONDS**
(Si cette garantie ne fait pas l'objet de cette demande, cocher ici ☐ et procéder à la prochaine question.)

(a) Par quel moyen effectuez-vous vos transferts de fonds?
☐ par télégramme; ☐ par voie électronique ; ☐ par reconnaissance vocale

(b) (i) Fréquence approximative des transferts?
(ii) Valeur moyenne (en dollars) des transferts? $
(iii) Valeurs maximale (en dollars) des transferts? $

(c) Qui est autorisé à effectuer des tranferts de fonds? (prière indiquer les postes)

(d) Est-ce que votre politique de transferts de fonds est développée de façon centrale et doit-elle être observée sans exception? Oui ☐ Non ☐

(e) Est-ce que toutes les instructions visant les transferts de fonds (qu'elles soient des instructions écrites ou des instuction verbales) sont authentifiées? Oui ☐ Non ☐

Si non, prière d'élaborer:

(f) Tous les transferts internes (y compris la paie) sont-ils dûment documentés et font-ils tous l'objet d'une approbation écrite de la part du directeur responsable? Oui ☐ Non ☐

(g) Exigez-vous sans exception une contreseignature pur tout transfert? Oui ☐ Non ☐

Si non, prière d'élaborer:

(h) Avant de procéder à un transfert de fonds, exigez-vous que votre institution financière vérifie l'authenitcité de la demande auprès d'un employé autre qu celui qui aura formulé Oui ☐ Non ☐

Dans l'affirmative, à partir de quel montant? $

(i) Avez-vous établi un protcole de rappel enregistré pour tout transfert de fonds? Oui ☐ Non ☐

Si non, prière d'élaborer:

(j) Procédez-vous à une conciliation des transferts au moins une fois par jour? Oui ☐ Non ☐

Si non, à quelle fréquence?

(k) Pour les clients autorisés à effectuer des transferts de fond à votre compte:
(i) jouissent-ils d'une autorisation écrite? Oui ☐ Non ☐
(ii) doivent-ils un NIP? Oui ☐ Non ☐
(iii) de telles autorisations, sont-elles enregistrées? Oui ☐ Non ☐
(iv) de telles autorisations font-elles l'objet d'un rappel de vérification? Oui ☐ Non ☐

(l) Qui (cocher la case appropriée) est susceptible d'effectuer des transferts de fonds de vive voix?
☐ clients; ☐ employés pour un client; ☐ autres (prière d'élaborer)

(m) Faute d'exifer des rappels pour fins de vérifications, quelles autres procédures de contrôle avez-vous établi quant aux transferts de fonds?

(n) Y a-t-il un manuel de procédures visant les transferts de fonds? Oui ☐ Non ☐

(o) Est-ce que les mêmes procédures sont en vigeur à tous les emplacements? Oui ☐ Non ☐

Si non, prière d'élaborer:

12. **FRAUDE TÉLÉPHONIQUE**
(Si cette garantie ne fait pas l'objet de cette demande, cocher ici ☐ et procéder à la prochaine question.)

(a) Qui est responsable de l'administation de votre système active par la voix? (Prière cocher la case appropriée)
a) ☐ personnel interne; b) ☐ personnel externe

(b) Nombre d'individus autorisés à utiliser le système informatique active par la voix?

Si plus qu'une personne, y a-t-il des identifications distinctes? Oui ☐ Non ☐

(c) Chaque utilisteur identifié en (b) ci-dessus, utilise-t-il un mot de passe? Oui ☐ Non ☐

(d) A quelle fréquence doit-on obligatoirement modifier son mot de passe?
☐ à chaque semaine; ☐ aux deux semaines ; ☐ au mois

(e) Quelles mesures de sécurité avez-vous instaurées afin de prevenir la fraude téléphonique?

13. **RESSOURCES HUMAINES**

(a) Vérifiez-vous les antécédents de tout postulant, y compris les antécédents d'emploi? Oui ☐ Non ☐

Dans l'affirmative, qui est chargé de cette tache?

(b) Avez-vous établi un procédure de sélection pour entrepreneurs, fournisseurs, employés temporaires et employés a temps partiel? Oui ☐ Non ☐

Dans l'affirmative, qui est chargé de cette tache?

Si non, de quelle façon déterminez-vous la qualification et la sélection de ceux-ci?

(c) Est-ce que des identifications sont émises à un nombre restreint de techniciens externes? Oui ☐ Non ☐

(d) Utlisez-vous les matériaux ou les services de logiciels de vos entrepreneurs? Oui ☐ Non ☐

Dans l'affirmative, prière d'élaborer:

(e) Est-ce que votre informaticien ou votre service de vérification effectue un vérification des mesures de sécurité et de protection mises en place par vos entrepreneurs? Oui ☐ Non ☐

Dan l'affirmative, à quelle fréquence?

(f) Tous les contrats, font-ils l'objet d'une vérification de la part de vois conseillers juridiqes et une copie est-elle remise au service de la sécurité informatique? Oui ☐ Non ☐

14. **PROTOCOLE ANTISINISTRE**

(a) Advenant le non fonctionnement de système principal, faites-vous l'essai du plan de secours de de sauvegarde des données? Oui ☐ Non ☐

(b) Le plan de secours exige-t-il que chaque emplacement effectue une évaluation detaillée du risque? Oui ☐ Non ☐

(c) Le plan de secours, fait-il l'objet d'une vérification et d'une mise à jour semestrielle (ou plus souvent advenant l'implementation des modifiactions majeures)? Oui ☐ Non ☐

Si non, prière d'élaborer:

15. **SINISTRES**

(a) Au cours de trois(3) dernière années, combien de fois a-t-on ciblé votre systèmes?

(b) D'après vous, ces attaques étaient de nature (cocher la case appropriée)
☐ aléatoire; ☐ aléatoire et ciblé; ☐ tous ciblés; ☐ sans objet

(c) En moyenne, ces attaques étaient découvertes à l'intérieur de combien de temps? (cocher la case appropriée)
☐ 15 minutes ou moins; ☐ 15 – 30 minutes; ☐ 30 – 60 minutes; ☐ plus que 60 minutes

(d) Au cour des trois (3) dernière années, à combien s'élève la totalité des pertes ou dommages encourus à la suite des attaques informatiques?
$

(e) Au cours de six (6) dernières années avez-vous soumis des réclamations (ou avis de perte potentielle) à tout Assureur en vertu d'une assurance contre la fraud informatique? Oui ☐ Non ☐

(f) Énumérez toutes les pertes (assurées ou non) au cours des six (6) dernières années se rapportant à une assurance similaire à celle qui fait l'objet demande:

Date du sinister	Nature du sinistre	Montant du sinsitre	Indemnisation des assurances	Détails du sinistre
		$	$	
		$	$	
		$	$	
		$	$	

Au cours des six (6) dernières années, vous a-t-on déjà refusé ou annulé une assurance similaire à celle qui fait l'objet de cette Proposition? Oui ☐ Non ☐

INFORMATIONS FRAUDULEUSES
Lorsque, sciemment et dans le but de frauder une compagnie d'assurance ou une autre personne, une personne soumet une proposition d'assurance renfermant de faux reseignements ou dissimule, dans le but d'induire en erreur, des reseignements concernant des faits importants à cet effet, elle commet alors un act frauduleux en matière d'assurance, ce qui constitute un délit.

MODIFICATIONS IMPORTANTES
Le soussigné declaré qu'au meilleur des ses connaissances, toutes les information fournies dans la présente propostion et dans tout proposition supplémentaire ou pièces jointes ont complètes, exactes et conformes à la vérité. Toute représentation frauduleuse, omission, dissimulation de faits ou fausse déclaration servira comme motifs pouvant mener à la résiliation de toute police émise sur la foi de telles information.

Si une modification importante était apportée au réponses présentées dans la proposition avant la prise d'effect de la police, le Preneur doit en aviser par écrit l'assureur et, à la seule discrétion de l'assureur, toute soumission proposée à la présente pourrait être modifée ou retirée.

AUTORISATION ET SIGNATURE
L'assureur et ses représentants son autorisés par les présentes à faire toute recherche et à mener toute enquête qu'ils jugeront nécessaires en rapport avec la présente proposition. Si une police est émise à la suite de cette demande, l'assureur est autorisé par les présentes à utilise et à divulguer à toute autorité, ou à ses avocats, ses affiliés associés ou représentants tout information quelconque qu'il jugera nécessaire a l'accomplessement de ses besoins en sa qualité d'assureur.

La signature de cette proposition n'engage ni l'assureur ni le Preneur à conclure un contrat d'assurance.

La présente proposition doit être signée par un dirigeant du Preneur, le gestionnaire des risques ou la personne responsable des assuances de l'entrepreise.

Daté à: ce jour de/d' 20

Signé par:

(Preneur) en caratères d'imprimerie

(Nom) en caratères d'imprimerie

(Titre) en caratères d'imprimerie

(Signature)