DEMANDE CYBERNÉTIQUE D'AXIS

AXIS REINSURANCE COMPANY (SUCCURSALE CANADIENNE)
70 York Street, Suite 1010, Toronto, ON. M5J 1S9
Téléphone : **(416) 361-7200** | Sans frais : **(866) 991-7141** | Télécopieur : **(416) 361-7225**

https://www.axiscapital.com/canada/insurance/cyber-technology-e-o

UNIQUEMENT EN CE QUI CONCERNE LES COUVERTURES DE RESPONSABILITÉ FONDÉES SUR LA DATE DES DEMANDES D'INDEMNISATION DANS LE CADRE DE LA POLICE POUR LAQUELLE LA PRÉSENTE PROPOSITION EST SOUMISE : CETTE POLICE D'ASSURANCE FOURNIT UNE COUVERTURE SUR LA BASE DE DEMANDES D'INDEMNISATION ET DE DÉCLARATIONS ET NE S'APPLIQUE QU'AUX DEMANDES D'INDEMNISATION FORMULÉES POUR LA PREMIÈRE FOIS À L'ENCONTRE DE L'ASSURÉ AU COURS DE LA PÉRIODE D'ASSURANCE OU DE TOUTE PÉRIODE DE DÉCLARATION ÉTENDUE APPLICABLE ET DÉCLARÉE À L'ASSUREUR COMME INDIQUÉ DANS LA SECTION DÉCLARATION DES DEMANDES D'INDEMNISATION ET DES ÉVÉNEMENTS LES FRAIS DE DÉFENSE SONT INCLUS DANS LES LIMITES DE L'ASSURANCE ET LEUR PAIEMENT ÉRODERA ET POURRA ÉPUISER LES LIMITES DE L'ASSURANCE.

NOUVELLE DEMANDE COMMERCIALE

- Le terme « Demandeur » désigne individuellement et collectivement tous les assurés proposés. Toutes les réponses sont réputées être faites au nom de tous les assurés proposés. **Si les réponses diffèrent pour les assurés proposés (y compris les filiales), veuillez remplir des annexes supplémentaires pour ces derniers.**
- La présente Demande et tous les documents qu'elle contient sont confidentiels.
- La soumission de la présente Demande n'oblige pas le demandeur à souscrire une assurance et l'assureur n'est pas tenu de vendre une assurance ou de proposer une assurance aux conditions spécifiques demandées.
- Si la police demandée est émise, la présente Demande, y compris toutes les propositions complémentaires et tous les documents et informations soumis dans le cadre de la présente Demande, sera considérée comme jointe à la police et en fera partie intégrante.

DIRECTIVES

- Répondez à toutes les questions de manière exhaustive, sans laisser de blancs. Vérifier les réponses lorsqu'elles sont demandées.
- Si l'espace est insuffisant, poursuivez les réponses sur votre papier à en-tête.
- La présente Demande doit être complétée, datée et signée par un agent autorisé de l'entité identifiée dans la section intitulée « Informations sur le demandeur » ci-dessous.

INFORMATIONS SUR LE DEMANDEUR

Nom du demandeur	
Adresse postale :	
Site(s) Web :	
Gestionnaire des risques Contact :	

Contact pour la réponse aux incidents :				
Activités commerciales :	Veuillez décrire les activités commerciales, les services et les produits du demandeur			
Revenues :	Recettes brutes annuelles prévues pour l'année fiscale en cours			
Recettes brutes annuelles de l'exercice précédent				
Coût d'exploitation :	Coût de fonctionnement annuel pour l'année fiscale en cours			
Dotation budgétaire de l'exercice en cours pour	TI :		La cybersécurité :	
Effectifs :	Employés :		Entrepreneurs :	
Travailler à distance :				
Les régions :	Pourcentage des recettes prévues dans chaque région où le demandeur exerce ses activités :			
% US	% Canada	% UK	% Europe	% AUS/NZ
% LATAM	% Russie	% MEA	% APAC	
Structure de la propriété	Catégorie décrivant le mieux la structure de l'actionnariat : Cochez toutes les cases qui s'appliquent			
☐ Sociétés cotées en bourse	☐ Privé	☐ Filiale	☐ Gouvernement	☐ Sans but lucratif

ACTIF

Informations personnelles	Aux fins de la présente demande, les informations personnelles sont les IIP, les IPS, les ICP et les informations biométriques décrites ci-dessous.
Pour chacun des types d'informations personnelles suivants, quel est le nombre approximatif de personnes dont les informations personnelles sont collectées, stockées, utilisées ou traitées par le demandeur ou par un tiers pour le compte du demandeur?	

PII	Informations à partir desquelles une personne peut être identifiée ou contactée de manière unique et fiable, ou qui sont utilisées pour authentifier une personne dans le cadre de transactions commerciales ou pour accéder à ses comptes ou à ses dossiers. (Nom de l'individu, adresse, adresse électronique, numéro de téléphone, passeport, sécurité sociale, permis de conduire ou autres numéros d'identification délivrés par le gouvernement, numéros de crédit, de débit ou autres numéros de comptes financiers, codes de sécurité, mots de passe, codes PIN et questions et réponses de sécurité)	
PHI	Informations sur la santé ou les soins médicaux d'une personne. (nom de la personne, dossiers médicaux, antécédents médicaux, factures médicales, résultats d'analyses de laboratoire, numéros de dossier médical, numéros de régime de santé ou de bénéficiaire de soins, identifiants de dispositifs médicaux et numéros de série)	
PCI	Informations sur la carte de paiement	
Biométrique	Caractéristiques physiques ou comportementales uniques d'un individu. (Empreintes digitales, empreintes faciales, scanners des mains, empreintes veineuses, empreintes vocales, scanners de l'iris ou de la rétine, frappes au clavier, démarche ou autres schémas physiques, données relatives au sommeil, à la santé ou à l'exercice physique, ADN ou marqueurs biologiques)	
Le demandeur vend-il ou partage-t-il des informations personnelles?		Oui ☐ Non ☐
Le demandeur stocke-t-il ou traite-t-il des informations personnelles pour le compte d'un tiers?		Oui ☐ Non ☐
Informations sur l'entreprise	Aux fins de la présente demande, les informations sur l'entreprise font référence à la propriété intellectuelle de tiers, aux actifs incorporels, aux secrets commerciaux, aux informations commerciales non publiques, telles que les informations financières privilégiées, les informations sur les fusions et acquisitions et sur le développement des activités ou des produits, les listes de clients, les projections et la stratégie de vente, ou les informations portant la mention « confidentiel ».	
Le demandeur stocke-t-il ou traite-t-il des informations sur les entreprises?		Oui ☐ Non ☐
Informations essentielles	Aux fins de la présente demande, les informations critiques désignent les systèmes, les logiciels, les programmes, les demandes et les informations qui sont essentielles à l'activité du demandeur.	
Veuillez décrire toute information considérée comme critique.		
Veuillez décrire les mesures de sécurité supplémentaires appliquées aux informations critiques		

Réseau	Le réseau du demandeur comprend-il les éléments suivants? Cochez toutes les cases qui s'appliquent			
☐ Applications Web	☐ Applications hébergées	☐ Systèmes POS	☐ Dispositifs personnels	☐ Appareils BYOD
☐ Terminaux de paiement (DAB)	☐ Supports amovibles (USB, stockage hors ligne)	☐ Systèmes embarqués dans les véhicules	☐ IoT critique (sécurité, incendie, BAS)	☐ OT/ICS/ SCADA
☐ Dispositifs de santé	☐ Dispositifs d'IA/robotiques			
Qui stockent ou traitent des Informations personnelles protégées, des informations d'entreprise ou des informations critiques, ou qui exécutent des processus commerciaux critiques? Cochez toutes les cases qui s'appliquent				
☐ Applications Web	☐ Applications hébergées	☐ Systèmes POS	☐ Dispositifs personnels	☐ Appareils BYOD
☐ Terminaux de paiement (DAB)	☐ Supports amovibles (USB, stockage hors ligne)	☐ Systèmes embarqués dans les véhicules	☐ IoT critique (sécurité, incendie, BAS)	☐ OT/ICS/ SCADA
☐ Dispositifs de santé	☐ Dispositifs d'IA/ robotiques			
Combien de serveurs se trouvent sur le réseau du demandeur?				
Où se trouvent les serveurs? Cochez toutes les cases qui s'appliquent				
☐ ÉTATS-UNIS	☐ Canada	☐ ROYAUME-UNI	☐ Europe	☐ AUS/NZ
☐ LATAM	☐ Russie	☐ MEA	☐ APAC	
Matériel TIV	Quelle est la valeur de remplacement approximative des ordinateurs de bureau et portables du demandeur et des dispositifs d'entrée/ sortie associés, des dispositifs mobiles et des réseaux, du stockage des données, des dispositifs de sauvegarde et des périphériques?			
Site Web	Le site Web du demandeur est-il essentiel à son activité quotidienne?			Oui ☐ Non ☐
Comment le site est-il géré?	☐ En interne	☐ Externalisé		
Les contractants ou les prestataires de services ont-ils des privilèges d'administrateur sur le site Web?				Oui ☐ Non ☐
Commentaires supplémentaires sur les actifs				

GOUVERNANCE

Responsable de la sécurité de l'information	Identifier la fonction la plus élevée de l'entreprise en matière de sécurité de l'information, telle que CISO (chief information security officer) ou CSO (chief security officer) ou l'équivalent fonctionnel.

Cette fonction a-t-elle une responsabilité directe dans la gestion de la réponse aux incidents de sécurité?	Oui ☐ Non ☐

De qui ce rôle relève-t-il? Cochez toutes les cases qui s'appliquent

☐ Dirigeants ou comité de dirigeants	☐ Conseil d'administration	☐ Principaux propriétaires ou actionnaires

Identifier tout autre	

Quelle est la fréquence des réunions d'information dans le cadre de cette fonction? Au moins :	☐ Semestriellement	☐ Annuellement

Responsable de la protection de la vie privée	Identifier la fonction la plus élevée de l'entreprise en matière de protection de la vie privée, telle que le CPO (chief privacy officer) ou le DPO (data protection officer) ou l'équivalent fonctionnel

Cette personne est-elle directement responsable de la gestion de la réponse aux incidents en matière de protection de la vie privée?	Oui ☐ Non ☐

De qui ce rôle relève-t-il? Cochez toutes les cases qui s'appliquent

☐ Dirigeants ou comité de dirigeants	☐ Conseil d'administration	☐ Principaux propriétaires ou actionnaires

Identifier tout autre	

Quelle est la fréquence des réunions d'information dans le cadre de cette fonction? Au moins :	☐ Semestriellement	☐ Annuellement

Politique de confidentialité	Le demandeur dispose-t-il d'une politique écrite en matière de protection de la vie privée ou d'une notice d'information sur la protection de la vie privée révisée par un avocat et mise à jour au moins une fois par an?	Oui ☐ Non ☐
Politique de sécurité de l'information	Le demandeur dispose-t-il d'une politique écrite en matière de sécurité de l'information?	Oui ☐ Non ☐
Quand cette politique a-t-elle été mise à jour pour la dernière fois?		

Est-il basé ou aligné sur l'une des normes, l'un des cadres ou l'une des meilleures pratiques suivantes? Cochez toutes les cases qui s'appliquent

☐ Cadre de cybersécurité du NIST ou autres publications	☐ ISO/IEC 27001	☐ US-CERT

Identifier tout autre	

Plan de continuité des activités	Le demandeur dispose-t-il d'un plan écrit de continuité des activités?		☐ Oui ☐ Non
À quelle fréquence ce plan est-il testé? Au moins :	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Plan de reprise après sinistre	Le demandeur dispose-t-il d'un plan écrit de reprise après sinistre?		☐ Oui ☐ Non
À quelle fréquence ce plan est-il testé? Au moins :	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Plan de réponse aux incidents	Le demandeur dispose-t-il d'un plan écrit d'intervention en cas d'incident?		☐ Oui ☐ Non
À quelle fréquence ce plan est-il testé? Au moins :	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement

Des copies des plans de continuité des activités, de reprise après sinistre et d'intervention en cas d'incident sont-elles stockées de manière à être accessibles si le réseau du demandeur devenait totalement indisponible?		☐ Oui ☐ Non
Conservation des documents et des archives	Le demandeur dispose-t-il d'une politique écrite de conservation des documents?	☐ Oui ☐ Non
	Le demandeur dispose-t-il d'une politique écrite en matière d'archivage?	☐ Oui ☐ Non

Ces politiques permettent-elles au demandeur d'identifier toutes les informations personnelles soumises aux activités suivantes au cours des 12 derniers mois? Cochez toutes les cases qui s'appliquent

☐ Collection	☐ Traitement	☐ Partage	☐ Vente	☐ Suppression

Ces politiques permettent-elles au demandeur d'identifier la ou les sources de collecte, de vente ou de partage des informations personnelles?	Oui ☐ Non ☐

Ces politiques permettent-elles au demandeur d'identifier le(s) but(s) commercial(aux) pour le(s)quel(s) les informations personnelles ont été collectées, vendues ou partagées?	Oui ☐ Non ☐
Commentaires supplémentaires sur la gouvernance	

CONFORMITÉ

Lois sur la protection de la vie privée	Le demandeur est-il actuellement en conformité avec les lois suivantes ou est-il en mesure de démontrer une position de conformité défendable en vertu de ces lois? Cochez toutes les cases qui s'appliquent			
☐ GDPR	☐ CCPA	☐ PIPEDA	☐ BIPA	☐ HIPAA/HITECH
☐ GLBA	☐ Règles FCRA/ FACTA/Red Flags	☐ TCPA	☐ CAN-SPAM	☐ VPPA
Identifier tout autre				
Traitement de l'information	En ce qui concerne les informations personnelles collectées, partagées ou vendues, le demandeur procède-t-il aux divulgations suivantes? Cochez toutes les cases qui s'appliquent			

☐ Avis public décrivant la collecte, le partage, la vente et l'utilisation	☐ Avis public décrivant les droits individuels concernant les informations personnelles, y compris le droit de restreindre la vente, la prise de décision automatisée ou d'autres traitements et le droit d'accès, de portabilité, de correction et d'effacement	☐ Avis individuel lors de la collecte décrivant le partage, la vente et l'utilisation
En ce qui concerne les informations personnelles collectées, partagées ou vendues, les processus suivants ont-ils été mis en place? Cochez toutes les cases qui s'appliquent		
☐ Accepter ou refuser la vente d'informations personnelles	☐ Demande de transfert de données personnelles	☐ Demande de correction des données personnelles
☐ Demande de suppression des données personnelles	☐ Demande d'informations sur des données personnelles spécifiques collectées, vendues ou partagées	
☐ Demande de limitation du traitement des données personnelles	☐ Demande de limitation de la prise de décision automatisée utilisant des informations personnelles	

Le demandeur recueille-t-il des informations biométriques auprès des groupes de personnes suivants? Cochez toutes les cases qui s'appliquent		
☐ Non collecté	☐ Employés/contractants	☐ Clients
Identifier tout autre		
En ce qui concerne les informations biométriques collectées, les divulgations et processus suivants sont-ils en place? Cochez toutes les cases qui s'appliquent		
☐ Avis public divulguant la collecte, l'utilisation, le traitement, le partage, la vente, le profit, la possession, la conservation, la sécurité et la destruction	☐ Avis individuel avant la collecte, y compris l'utilisation, le traitement, le partage, la vente, le profit, la possession, la conservation, la sécurité et la destruction	
☐ Consentement individuel ou libération pour la collecte, l'utilisation, le traitement, le partage, la vente, le profit, la possession, la conservation et la destruction, par écrit et revue par un avocat	☐ Avis individuel avant la collecte, y compris l'utilisation, le traitement, le partage, la vente, le profit, la possession, la conservation, la sécurité et la destruction	
☐ Politique écrite concernant la collecte, l'utilisation, le traitement, le partage, la vente, le profit, la possession, le stockage, la conservation et la destruction, conforme aux normes en vigueur dans le secteur d'activité du demandeur, examinée par un avocat et accessible au public		☐ Non collecté
Où sont stockées les informations biométriques? Cochez toutes les cases qui s'appliquent	☐ Nuage	☐ Réseau du demandeur
Les informations biométriques sont-elles soumises aux mesures suivantes? Cochez toutes les cases qui s'appliquent		☐ Cryptage en transit
☐ Chiffrement au repos	☐ Accès restreint sur la base du principe du moindre privilège	☐ Séparés dans un environnement isolé
Les produits ou services du demandeur sont-ils utilisés pour la collecte, l'utilisation, le traitement, le partage, la vente, le profit, la possession, la conservation ou la destruction d'informations biométriques?		☐ Oui ☐ Non

Veuillez décrire	
Le demandeur transmet-il des informations personnelles à l'étranger, dans une autre juridiction?	☐ Oui ☐ Non

Le demandeur respecte-t-il toutes les lois relatives à la transmission transfrontalière d'informations personnelles vers une autre juridiction?		☐ Oui ☐ Non
PCI DSS	Le demandeur est-il tenu de se conformer à la norme PCI DSS?	☐ Oui ☐ Non
Niveau marchand PCI (1-4) :		
Combien de transactions par carte de paiement le demandeur traite-t-il par an?		
Le demandeur est-il actuellement en conformité avec les exigences de la norme PCI DSS pour son niveau de commerçant?		☐ Oui ☐ Non
Quelle version de la norme PCI-DSS a été évaluée pour le demandeur?		
Commentaires supplémentaires sur la conformité		

CONTRÔLES

Maintenance	À quelle fréquence le demandeur met-il à jour les logiciels, corrige-t-il les vulnérabilités, désactive-t-il les services inutiles et supprime-t-il les logiciels et le matériel inutiles? Au moins :			☐ En continu
☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement

Veuillez donner un aperçu du processus et du calendrier de gestion des vulnérabilités et des correctifs critiques du demandeur, s'ils ne figurent pas dans la liste ci-dessous :				
Cible de correctifs critiques :	☐ < 24 heures	☐ 24-72 heures	☐ 3-7 jours	☐ > 7 jours
Cible de correctifs pour la gestion normale des vulnérabilités :	☐ <7 jours	☐ 7-14 jours	☐ 14-30 jours	☐ >30 jours
Quelle est la rapidité de mise en œuvre des mises à jour critiques après leur publication? Au moins à l'intérieur :				
☐ 24 heures	☐ 72 heures	☐ 1 semaine	☐ 2 semaines	☐ 1 mois

Gestion du cycle de vie et des stocks	Le demandeur utilise-t-il un système d'exploitation, du matériel ou des logiciels qui ne sont plus pris en charge ou qui sont considérés comme étant en fin de vie par le fabricant?	☐ Oui ☐ Non
Dans l'affirmative, veuillez donner un aperçu de l'utilisation, des plans d'assainissement, de la stratégie de déclassement, de la ségrégation et de tout autre contrôle ou garantie supplémentaire en place		

Quel est le pourcentage de matériel connecté au réseau qui est inventorié?			%
À quelle fréquence l'inventaire du matériel est-il mis à jour? Au moins :			
☐ En continu	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Quel est le pourcentage de logiciels connectés au réseau qui sont inventoriés?			%

Surveillance des journaux	Veuillez décrire les politiques d'enregistrement des audits, les pratiques d'examen des anomalies et les solutions d'analyse des journaux, telles que SIEM.

Ces politiques, pratiques et solutions sont-elles appliquées aux éléments suivants? Cochez toutes les cases qui s'appliquent		☐ Pare-feu	☐ Détection et prévention des intrusions	
La journalisation locale est-elle effectuée pour chaque hôte?				☐ Oui ☐ Non
Les journaux locaux sont-ils centralisés dans un système de gestion des journaux?				☐ Oui ☐ Non
À quelle fréquence les journaux sont-ils audités? Au moins :				☐ En continu
☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Combien de temps les journaux d'audit sont-ils conservés? Au moins :		☐ 30 jours	☐ 90 jours	☐ 1 an

Configuration de la sécurité	Le demandeur applique-t-il une gestion stricte de la configuration de la sécurité des dispositifs personnels, des applications Web, des serveurs, des bases de données et des applications critiques pour l'entreprise et la sécurité?	☐ Oui ☐ Non
À quelle fréquence ces configurations de sécurité sont-elles mises à jour? Au moins :		☐ En continu

☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Veuillez décrire les techniques de renforcement des systèmes mises en œuvre par le demandeur.				
L'installation de logiciels est-elle automatiquement contrôlée et les logiciels non autorisés sont-ils bloqués?				☐ Oui ☐ Non
Tests et analyses	Le demandeur effectue-t-il régulièrement des tests de pénétration?			☐ Oui ☐ Non
Quelle est la fréquence de ces tests? Au moins :				
☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement	☐ Tous les deux ans
Ces tests sont-ils réalisés en interne ou externalisés?				☐ Oui ☐ Non
Le demandeur procède-t-il régulièrement à des analyses de vulnérabilité?				☐ Oui ☐ Non
Quelle est la fréquence de cette analyse? Au moins :				☐ En continu
☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Sauvegardes	Le demandeur effectue-t-il des sauvegardes régulières de ses données?			☐ Oui ☐ Non
À quelle fréquence les informations critiques sont-elles sauvegardées? Au moins :			☐ En continu	☐ Quotidiennement
☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement
Lequel des éléments suivants, le demandeur utilise-t-il pour les sauvegardes?			Bandes	☐ Oui ☐ Non
Disques	☐ Oui ☐ Non		Nuage	☐ Oui ☐ Non
Où sont stockées les sauvegardes? Cochez toutes les cases qui s'appliquent			MSSP	☐ Oui ☐ Non
Sur place	☐ Oui ☐ Non		Stockage hors ligne	☐ Oui ☐ Non
Stockage hors site	☐ Oui ☐ Non		Centre de données secondaires	☐ Oui ☐ Non
Veuillez donner un aperçu de la stratégie de sauvegarde du demandeur et indiquer qui a accès à la sauvegarde				
Les sauvegardes sont-elles soumises aux mesures suivantes?				

Authentification multi-facteurs	☐ Oui ☐ Non	Cryptage	☐ Oui ☐ Non
Segmentation	☐ Oui ☐ Non	Analyse des virus et des logiciels malveillants	☐ Oui ☐ Non
Immuable	☐ Oui ☐ Non	Gestion des accès privilégiés	☐ Oui ☐ Non
Identifier les éventuels contrôles/sécurités supplémentaires			

Identifiants de sauvegarde uniques, stockés séparément des autres identifiants de l'utilisateur				☐ Oui ☐ Non
Si les sauvegardes sont chiffrées, les clés de chiffrement sont-elles stockées hors ligne?				☐ Oui ☐ Non
À quelle fréquence les sauvegardes sont-elles effectuées dans un lieu de stockage hors site? Au moins :	☐ Quotidiennement	☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle
À quelle fréquence les sauvegardes sont-elles effectuées dans un espace de stockage hors ligne? Au moins :	☐ Quotidiennement	☐ Hebdomadaire	☐ Mensuel	☐ Trimestrielle
À quelle fréquence une récupération complète à partir d'une sauvegarde est-elle testée? Au moins :	☐ Mensuel	☐ Trimestrielle		☐ Annuellement
Redondance	Le demandeur recourt-il à la redondance des systèmes d'entreprise critiques?			☐ Oui ☐ Non
Détection et prévention des intrusions	Le demandeur utilise-t-il une solution de détection et de prévention des intrusions?			☐ Oui ☐ Non
À quelle fréquence les journaux d'intrusion sont-ils examinés? Au moins :	☐ En continu			☐ Quotidiennement
☐ Hebdomadaire	☐ Bihebdomadaire	☐ Mensuel		☐ Trimestrielle
Quel est le délai prévu pour réagir à une intrusion?	Heures			Minutes

Détection et réponse aux points finaux	Le demandeur utilise-t-il une solution de détection et de réponse des points finaux (EDR)?	☐ Oui ☐ Non
Dans l'affirmative, l'une des solutions suivantes est-elle utilisée? Cochez toutes les cases qui s'appliquent.		
Si oui, quel est le pourcentage des terminaux du demandeur sur lesquels l'EDR est déployé?		%
Si oui, sur quel pourcentage des serveurs du demandeur la gestion électronique des données est-elle déployée?		%
Veuillez identifier la ou les solution(s) EDR en place, y compris les noms des sociétés et des produits :		

Prévention de la perte de données	Le demandeur utilise-t-il une solution de prévention des pertes de données? Veuillez décrire		
Le demandeur contrôle-t-il la transmission d'informations personnelles, d'informations sur l'entreprise et d'informations critiques en dehors du réseau? Cochez toutes les cases qui s'appliquent			☐ Hors réseau ☐ Supports amovibles
Les dispositifs de stockage amovibles sont-ils contrôlés et réglementés?			☐ Oui ☐ Non
Logiciel d'atténuation	L'un des éléments suivants a-t-il été mis en œuvre? Cochez toutes les cases qui s'appliquent		
☐ Atténuation des DDoS	☐ Logiciel de détection des logiciels criminels	☐ Logiciel anti-virus/anti-malveillant	
Cryptage	Le demandeur utilise-t-il un système de cryptage obligatoire pour protéger les éléments suivants? Cochez toutes les cases qui s'appliquent		
☐ Informations personnelles en transit		☐ Données personnelles au repos	
☐ Informations sur les entreprises en transit		☐ Informations sur l'entreprise au repos	
☐ Informations essentielles	☐ Dispositifs personnels	☐ Supports amovibles	
Filtration	Le demandeur utilise-t-il l'une des solutions suivantes?	SPF	☐ Oui ☐ Non
DKIM	☐ Oui ☐ Non	DMARC	☐ Oui ☐ Non

Pare-feu	Le demandeur utilise-t-il les pare-feux suivants? Cochez toutes les cases qui s'appliquent	☐ Extérieur ou périmètre	☐ Interne
Chaque pare-feu est-il protégé par un mot de passe?			☐ Oui ☐ Non
Le filtrage IP est utilisé pour empêcher les connexions à partir d'adresses malveillantes connues			☐ Oui ☐ Non
Les ports réseau ne peuvent être ouverts qu'en cas de besoin professionnel légitime			☐ Oui ☐ Non
L'accessibilité des ports est régulièrement vérifiée automatiquement			☐ Oui ☐ Non
Identifier tous les rôles ayant accès à la configuration des pare-feux ou au contrôle du trafic à travers les pare-feux?			

À quelle fréquence la configuration du pare-feu est-elle revue? Au moins :			☐ Semestriellement	☐ Annuellement
À quelle fréquence le micrologiciel du pare-feu est-il mis à jour? Au moins :			☐ Semestriellement	☐ Annuellement
Quelle est la politique en matière de pare-feu? Cochez toutes les cases qui s'appliquent		☐ Refuser tout par défaut, autoriser par exception		☐ Refus par exception
Ségrégation	Le demandeur a-t-il appliqué la segmentation du réseau dans son environnement?			☐ Oui ☐ Non
Si oui, veuillez indiquer sur quelle base :	Géographie	☐ Oui ☐ Non	Criticité du système	☐ Oui ☐ Non
	Filiales	☐ Oui ☐ Non	Emplacements de briques et de mortier	☐ Oui ☐ Non
	Fonction de l'entreprise	☐ Oui ☐ Non	Classification des données	☐ Oui ☐ Non
Tout autre détail/point à clarifier concernant la segmentation du réseau :				

Les éléments suivants sont-ils séparés dans un environnement isolé? Cochez toutes les cases qui s'appliquent				
☐ Informations personnelles	☐ Informations sur l'entreprise	☐ Serveurs critiques	☐ Informations essentielles	
Le développement, les essais et la production sont-ils effectués dans des environnements distincts?				☐ Oui ☐ Non
Accès	L'accès au réseau est-il limité sur la base du principe du moindre privilège?			☐ Oui ☐ Non
L'accès aux informations personnelles, aux informations de l'entreprise et aux informations critiques, est-il limité sur la base du principe du moindre privilège?				☐ Oui ☐ Non

L'accès est-il contrôlé et mis à jour? Au moins :				☐ En continu
☐ Quotidiennement	☐ Hebdomadaire	☐ Bihebdomadaire	☐ Mensuel	☐ Trimestrielle
L'exercice des droits d'administrateur et d'accès privilégiés fait-il l'objet d'un audit et d'une mise à jour? Au moins :				☐ En continu
☐ Quotidiennement	☐ Hebdomadaire	☐ Bihebdomadaire	☐ Mensuel	☐ Trimestrielle
Les modifications apportées aux comptes d'administrateur sont-elles signalées automatiquement?				☐ Oui ☐ Non
Tous les comptes sont-ils associés à des processus légitimes ou à des utilisateurs actuels?				☐ Oui ☐ Non
L'activité du demandeur consiste-t-elle à surveiller tous les accès privilégiés et les accès administrateurs pour détecter des comportements inhabituels?				☐ Oui ☐ Non
Le demandeur impose-t-il des exigences de sécurité minimales à tous les dispositifs se connectant au réseau?				☐ Oui ☐ Non
Le demandeur est-il en mesure d'effacer à distance les dispositifs personnels qui font partie de son réseau?				☐ Oui ☐ Non

Veuillez décrire les politiques de force, d'expiration et de réutilisation des mots de passe employés par le demandeur :	

L'authentification multifactorielle est-elle requise pour les accès suivants?			Informations essentielles	☐ Oui	☐ Non
Accès à distance	☐ Oui	☐ Non	Accès des tiers/fournisseurs	☐ Oui	☐ Non
Dispositifs personnels	☐ Oui	☐ Non	Informations et applications non critiques	☐ Oui	☐ Non
Le demandeur utilise-t-il un outil de gestion des accès privilégiés (PAM)?				☐ Oui	☐ Non
Si oui, l'accès à l'outil PAM est-il soumis à l'authentification multifactorielle?				☐ Oui	☐ Non

Dans la négative, veuillez décrire comment le demandeur sécurise les comptes privilégiés et les comptes d'administrateur :

Quelle méthode de facteur secondaire le demandeur utilise-t-il pour l'authentification multifactorielle?	SMS	☐ Oui	☐ Non
	Dispositif non corporatif (si oui ci-dessus)	☐ Oui	☐ Non

Authentification biométrique ☐ Oui ☐ Non	Demande d'authentification ☐ Oui ☐ Non	Courriel secondaire ☐ Oui ☐ Non	Certificat de point final ☐ Oui ☐ Non	Clés de sécurité physique ☐ Oui ☐ Non

Identifiez-en d'autres :	
Veuillez indiquer le nombre de comptes de domaine et de service que le demandeur possède dans le groupe d'administration du domaine :	

Sont-ils stockés dans l'un ou l'autre des endroits suivants?	Annuaire local	☐ Oui ☐ Non	Active Directory	☐ Oui ☐ Non

Identifiez-en d'autres :	
L'utilisation et la distribution de l'accès administrateur et privilégiée nécessitent-elles l'approbation de la direction générale?	☐ Oui ☐ Non

Veuillez décrire les politiques de sécurité sans fil du demandeur :					
Les connexions à partir d'appareils sans fil non fiables sont-elles autorisées?					☐ Oui ☐ Non
Les appareils sans fil non fiables utilisent-ils un réseau distinct?					☐ Oui ☐ Non
Formation et sensibilisation	Le demandeur organise-t-il au moins une fois par an une formation obligatoire à la sécurité de l'information et à la protection de la vie privée à l'intention de ses employés et de ses sous-traitants dans les domaines suivants?				
Ingénierie sociale	☐ Oui ☐ Non	Campagnes d'hameçonnage	☐ Oui ☐ Non		
Formation basée sur les rôles	☐ Oui ☐ Non	Conformité en matière de protection de la vie privée et de traitement des données	☐ Oui ☐ Non		
Sensibilisation à la sécurité et aux menaces			☐ Oui ☐ Non		
Identifier tout autre					
Des simulations d'hameçonnage sont-elles organisées pour tous les employés?					☐ Oui ☐ Non
À quelle fréquence le demandeur organise-t-il des simulations d'hameçonnage?	☐ Mensuel	☐ Trimestrielle	☐ Semestriellement	☐ Annuellement	
Les simulations d'hameçonnage :	Basé sur le rôle ☐ Oui ☐ Non	Ciblé ☐ Oui ☐ Non	Envoyé de manière échelonnée ☐ Oui ☐ Non		
Taux de clics de la simulation la plus récente	☐ < 5 %	☐ 5-10 %	☐ 10-15 %	☐ 15-20 %	☐ > 20 %
Taux de déclaration de la simulation la plus récente :	☐ < 5 %	☐ 5-10 %	☐ 10-15 %	☐ 15-20 %	☐ > 20 %
Le demandeur dispose-t-il d'un module complémentaire de signalement des courriels d'hameçonnage activé pour tous les utilisateurs de la messagerie électronique?					☐ Oui ☐ Non
Le demandeur utilise-t-il une solution de sandboxing pour enquêter sur les courriels et les pièces jointes suspects?					☐ Oui ☐ Non
Comment le demandeur traite-t-il les récidivistes/les cliqueurs?					
Le demandeur met-il à jour au moins une fois par an le contenu de sa formation à la sécurité de l'information et à la protection de la vie privée, ainsi que ses communications?					☐ Oui ☐ Non

Le demandeur exige-t-il des prestataires de services et des tiers ayant accès au réseau et aux données du demandeur qu'ils suivent au moins une fois par an une formation à la sécurité de l'information et à la protection de la vie privée?			☐ Oui ☐ Non
Dépistage	Les demandeurs à un emploi font-ils l'objet d'une vérification, notamment de leurs antécédents en matière de crédit, de leur casier judiciaire et d'un dépistage de drogues, dans les limites autorisées par la loi?		☐ Oui ☐ Non
Groupes de partage entre pairs	Le demandeur participe-t-il à un programme de partage des menaces, des vulnérabilités et des incidents en matière de sécurité de l'information afin d'améliorer la sensibilisation, l'évaluation, la surveillance et la réaction?		☐ Oui ☐ Non
Vol et perte physique	Le demandeur détecte-t-il le retrait du matériel critique du réseau?		☐ Oui ☐ Non
Le demandeur applique-t-il une procédure de signalement et d'enregistrement du matériel perdu ou volé?			☐ Oui ☐ Non
Gestion de la sécurité	L'un des éléments suivants a-t-il été mis en œuvre? Cochez toutes les cases qui s'appliquent		
☐ Gestion unifiée des menaces ou systèmes de prévention des menaces	☐ Audit ou évaluation indépendante de la sécurité	☐ Services de sécurité gérés	
Le demandeur dispose-t-il d'un centre d'opérations de sécurité (SOC)?			☐ Oui ☐ Non
Dans l'affirmative :	Est-il surveillé 24 heures sur 24 et 7 jours sur 7?		☐ Oui ☐ Non
	Est-il géré en interne ou par un tiers?	En interne	☐ Oui ☐ Non
	Tiers ☐ Oui ☐ Non	Hybride	☐ Oui ☐ Non
Fournir toute autre information sur le SOC du demandeur			
Le demandeur utilise-t-il Microsoft (Office) 365?			☐ Oui ☐ Non
Dans l'affirmative, les mesures suivantes sont-elles mises en œuvre?			
Microsoft 365 Advanced Threat Protection (ATP)/ Defender	☐ Oui ☐ Non	Authentification multi-facteurs pour tous les utilisateurs de Microsoft 365	☐ Oui ☐ Non
Le protocole de bureau à distance (RDP) est-il activé?			☐ Oui ☐ Non
Si oui, le RDP est-il accessible?			
En interne	☐ Oui ☐ Non	À l'extérieur	☐ Oui ☐ Non
Dans l'affirmative, les mesures suivantes sont-elles mises en œuvre?			

Accès RPV avec authentification multifactorielle uniquement	☐ Oui ☐ Non	Authentification multi-facteurs pour l'accès	☐ Oui ☐ Non
Authentification au niveau du réseau activée	☐ Oui ☐ Non	Accessible via PAM	☐ Oui ☐ Non
Identifier tout autre contrôle/sécurité en place pour l'utilisation de RDP :			
Commentaires supplémentaires sur les contrôles			

CONTINUITÉ DES ACTIVITÉS

Délai de récupération	En cas d'interruption du réseau du demandeur, quel est l'objectif du demandeur en matière de délai de rétablissement des systèmes, applications et processus critiques? Tout au plus :			
☐ <8 heures	☐ 8-12 heures	☐ 12-24 heures	☐ 24-48 heures	☐ >48 heures
Ont-ils été validés au cours des 12 derniers mois?				☐ Oui ☐ Non
Impact	En cas d'indisponibilité d'informations critiques ou de systèmes, d'applications ou de processus critiques, combien de temps faudrait-il pour interrompre de manière significative les activités du demandeur? Tout au plus :			
☐ <1 heure	☐ 1 à 8 heures	☐ 8-12 heures	☐ 12-24 heures	☐ 24-48 heures
Le demandeur est-il en mesure de recourir à une solution de rechange manuelle en cas d'interruption du réseau?				☐ Oui ☐ Non
Veuillez décrire				

Le demandeur est-il en mesure de basculer immédiatement dans un système d'information redondant en cas d'interruption du réseau?	☐ Oui ☐ Non
Veuillez décrire	

Le demandeur dispose-t-il d'une installation informatique de secours sur site chaud, tiède ou froid?		☐ Oui ☐ Non
Veuillez décrire		
Événement antérieur	Le demandeur a-t-il subi une interruption partielle ou totale de son réseau pendant plus de 8 heures?	☐ Oui ☐ Non

LES PRESTATAIRES DE SERVICES

Services informatiques et services en nuage	Identifier tous les services informatiques et basés sur le nuage qui fournissent des applications, des infrastructures ou des processus critiques pour l'entreprise. Cochez toutes les cases qui s'appliquent			
☐ Adobe	☐ AWS	☐ Dropbox	☐ Google	☐ IBM
☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle	☐ Rackspace	☐ Salesforce
☐ SAP	☐ Jour ouvrable	☐ Xero	☐ Zoho	
Identifier tout autre				

Services non informatiques	Identifier les cinq fournisseurs de services non informatiques qui assurent les processus commerciaux les plus critiques pour l'activité du demandeur.
1	2
3	4
5	

Le demandeur examine-t-il les contrôles de sécurité des informations et de protection de la vie privée de chacun de ses fournisseurs de services informatiques, en nuage et non informatiques?	☐ Oui ☐ Non
Le demandeur vérifie-t-il les contrôles de la sécurité des informations et de la protection de la vie privée de chacun de ses fournisseurs de services informatiques, de services en nuage et de services non informatiques?	☐ Oui ☐ Non
Quelle est la fréquence des audits?	☐ Semestriellement ☐ Annuellement
L'accès du Prestataire de services au réseau ou aux données du demandeur est-il limité sur la base du principe du moindre privilège?	☐ Oui ☐ Non
Veuillez décrire toute autre restriction concernant l'accès du fournisseur de services au réseau ou aux données :	
L'accès du Prestataire de services aux données ou au réseau du demandeur est-il contrôlé?	☐ Oui ☐ Non
Quelle est la fréquence des examens? Au moins :	☐ En continu
☐ Hebdomadaire ☐ Mensuel ☐ Trimestrielle ☐ Semestriellement	☐ Annuellement
Contrats — Le demandeur a-t-il conclu des accords écrits avec tous les tiers ayant accès au réseau ou aux données du demandeur?	☐ Oui ☐ Non
Tous les accords écrits exigent-ils que le tiers défende ou indemnise le demandeur en cas de responsabilité liée à un incident de sécurité ou de confidentialité sur le réseau du tiers ou causé par le tiers?	☐ Oui ☐ Non
Tous les accords écrits exigent-ils que le tiers souscrive une assurance applicable au demandeur en cas d'incident lié à la sécurité ou à la protection de la vie privée sur le réseau du tiers ou causé par ce dernier?	☐ Oui ☐ Non
L'un des accords écrits limite-t-il la responsabilité du tiers en cas d'incident lié à la sécurité ou à la protection de la vie privée sur le réseau du tiers?	☐ Oui ☐ Non

Commentaires supplémentaires sur les prestataires de services	

CRIME

Transactions	Quel est le nombre moyen quotidien d'opérations de transfert de fonds de première partie?	
Quelle est la valeur moyenne transférée chaque jour?		
Quelle est la valeur moyenne d'un transfert?		
Authentification et approbation de niveau supérieur	Le demandeur utilise-t-il un protocole pour confirmer les instructions de transfert, y compris un rappel, un courriel ou une autre méthode d'authentification de l'instruction?	☐ Oui ☐ Non
Veuillez décrire		
Le demandeur utilise-t-il un protocole nécessitant plus d'une approbation ou une approbation de niveau supérieur?		☐ Oui ☐ Non
Veuillez décrire		
Formation à la lutte contre la fraude	Le demandeur organise-t-il au moins une fois par an une formation à la lutte contre la fraude à l'intention de ses employés?	☐ Oui ☐ Non

Événements antérieurs	Au cours des trois dernières années, le demandeur a-t-il été victime d'un transfert frauduleux ou d'instructions de transfert, d'ingénierie sociale, d'une compromission du courrier électronique professionnel ou d'une attaque par hameçonnage?	☐ Oui ☐ Non
Commentaires supplémentaires sur la criminalité		

MÉDIA

Activités médiatiques :	Veuillez décrire les activités médiatiques du demandeur, y compris les activités publicitaires		
Allocation du budget de l'année fiscale en cours aux activités publicitaires :			
Contenu du site Web	Quel type de contenu le demandeur publie-t-il ou affiche-t-il sur son site Web? Cochez toutes les cases qui s'appliquent		☐ Pas de site Web
☐ Contenu créé par le demandeur	☐ Contenu de tiers sous licence	☐ Contenu de tiers sans licence (forums de discussion, critiques)	☐ Diffusion en continu de vidéos ou de musique
Examen et approbation juridique	Le contenu est-il revu par un avocat avant d'être publié ou affiché sur un site Web détenu ou exploité par le demandeur ou sur ses pages de médias sociaux ou sous ses comptes sur des sites Web de tiers?		☐ Oui ☐ Non
L'examen de l'avocat porte-t-il sur les risques de responsabilité suivants? Cochez toutes les cases qui s'appliquent			
☐ Diffamation ou dénigrement	☐ Outrage ou détresse émotionnelle	☐ Atteinte à la vie privée ou aux droits de la personnalité	☐ Violation des droits d'auteur, plagiat ou détournement d'idées
Le demandeur dispose-t-il d'une procédure pour traiter les allégations selon lesquelles le contenu créé, affiché ou publié par le demandeur est diffamatoire ou dénigrant ou porte atteinte aux droits d'auteur ou au droit à la vie privée de tiers?			☐ Oui ☐ Non
Le demandeur dispose-t-il d'une politique écrite pour traiter les demandes de rétractation ou de correction?			☐ Oui ☐ Non

Le demandeur dispose-t-il d'une politique écrite pour vérifier l'exactitude et l'originalité du contenu créé par le demandeur ou en son nom?		☐ Oui ☐ Non
Contrats	Le demandeur a-t-il conclu des accords écrits avec tous les tiers qui fournissent des services publicitaires ou du contenu au demandeur ou en son nom?	☐ Oui ☐ Non
Tous les accords écrits exigent-ils que le tiers défende ou indemnise le demandeur en cas de responsabilité découlant des services ou du contenu du tiers?		☐ Oui ☐ Non
Tous les accords écrits exigent-ils que le tiers souscrive une assurance applicable au demandeur en cas de responsabilité découlant des services ou du contenu du tiers?		☐ Oui ☐ Non

L'un des accords écrits limite-t-il la responsabilité du tiers en ce qui concerne les services ou le contenu du tiers?	☐ Oui ☐ Non
Commentaires supplémentaires sur les médias	

DEMANDES D'INDEMNISATION ET ÉVÉNEMENTS RELATIFS À LA SÉCURITÉ ET À LA PROTECTION DE LA VIE PRIVÉE

Divulgation non autorisée	Au cours des trois dernières années, le demandeur a-t-il été confronté à une défaillance dans la protection des informations personnelles ou des informations de l'entreprise dont le demandeur ou son Prestataire de services a la charge, la garde ou le contrôle, ou dont le demandeur est légalement responsable? (dommages, destruction, perte, vol, divulgation non autorisée)	☐ Oui ☐ Non
Veuillez décrire		

Collecte, conservation, utilisation ou traitement illicites	Au cours des trois dernières années, le demandeur a-t-il été informé d'une demande d'indemnisation, d'une plainte ou d'une demande alléguant la violation d'un droit à la vie privée ou le non-respect d'une Réglementation en matière de protection de la vie privée concernant des données à caractère personnel dont le demandeur ou son Prestataire de services a la charge, la garde ou le contrôle, ou dont le demandeur est légalement responsable? (collecte, conservation, vente, élimination, suppression, divulgation, utilisation, contrôle, traitement, accès ou correction illicites)	☐ Oui ☐ Non
Veuillez décrire		

Accès non autorisé	Au cours des trois dernières années, le demandeur a-t-il connu une défaillance de la sécurité de son réseau? (intrusion, altération, attaque par déni de service, insertion de virus, de logiciels malveillants, de logiciels rançonneurs ou d'autres Codes malveillants, demande d'extorsion ou autre accès ou utilisation non autorisé)	☐ Oui ☐ Non
Au cours des trois dernières années, le Demandeur a-t-il été informé d'une demande d'indemnisation, d'une plainte ou d'une demande alléguant ou découlant d'une défaillance de la sécurité de son réseau?		☐ Oui ☐ Non
Veuillez décrire		
Mesures réglementaires antérieures	Au cours des trois dernières années, le demandeur a-t-il fait l'objet d'une procédure civile ou administrative, d'une enquête civile, d'une citation à comparaître ou d'une demande d'informations de la part d'une agence gouvernementale, d'un organisme de protection des données ou d'une autre organisation ayant le pouvoir d'appliquer une Réglementation en matière de protection de la vie privée?	☐ Oui ☐ Non
Veuillez décrire		
Connaissances préalables	Un administrateur, un dirigeant ou un employé du demandeur, de sa société mère ou de l'une de ses filiales ou sociétés affiliées a-t-il connaissance d'un fait, d'une circonstance, d'un incident, d'un événement ou d'une transaction susceptible de donner lieu à une demande d'indemnisation, une plainte ou une demande alléguant un incident lié à la protection de la vie privée ou à la sécurité ou une responsabilité des médias, ou dispose-t-il d'informations à ce sujet?	☐ Oui ☐ Non

Veuillez décrire		
Avis préalable	L'une de ces questions a-t-elle été signalée à un autre assureur?	☐ Oui ☐ Non
Remédiation	En réponse à l'une de ces questions, le demandeur a-t-il entrepris ou achevé de modifier ses pratiques en matière de sécurité et de traitement des réseaux et des informations, ou d'autres changements, afin de remédier aux effets de la question ou de supprimer une vulnérabilité à l'origine de la question?	☐ Oui ☐ Non
Veuillez décrire		

DÉCLARATIONS ET SIGNATURE

En signant le présent document, le représentant autorisé soussigné du demandeur déclare, au nom de toutes les personnes et entités proposées pour la couverture, après enquête, qu'à sa connaissance :

1. Les déclarations et les réponses données dans la présente Demande, ainsi que tous les documents qui y sont joints, sont véridiques, exacts et complets.
2. Aucun fait ou information important pour le risque proposé à l'assurance n'a pas été déformé ou dissimulé.
3. Ces déclarations constituent une incitation matérielle pour l'assureur à fournir une proposition d'assurance.
4. Toute police émise par l'assureur le sera sur la base de ces déclarations.
5. Le demandeur signale immédiatement par écrit à l'assureur tout changement important dans ses activités, produits et services.
6. Le proposant signalera immédiatement par écrit à l'assureur toute modification importante des réponses fournies dans la présente Demande qui survient ou est découverte entre la date de la présente Demande et la date d'entrée en vigueur de la police pour laquelle une couverture est demandée en soumettant la présente Demande.
7. L'assureur se réserve le droit, dès réception d'un tel avis, de modifier ou de retirer toute proposition d'assurance qu'il a offerte.

AVERTISSEMENT

VEUILLEZ PRENDRE CONNAISSANCE DE LA DÉCLARATION DE FRAUDE DE L'ÉTAT FIGURANT À LA FIN DE LA PRÉSENTE DEMANDE, APPLICABLE À L'ÉTAT DANS LEQUEL LE DEMANDEUR RÉSIDE.

Toute personne qui, dans l'intention de frauder ou de faciliter sciemment une fraude à l'encontre de l'assureur, soumet une demande ou dépose une demande d'indemnisation contenant une déclaration fausse ou trompeuse, peut se rendre coupable de fraude à l'assurance.

La présente Demande doit être signée par le directeur général, le directeur financier, le directeur des opérations ou le directeur juridique du demandeur, ou leur équivalent fonctionnel, à moins que l'assureur ne donne des instructions contraires au demandeur.

Nom		Nom (signature)	
Titre		Date	

À REMPLIR PAR LES PRODUCTEURS UNIQUEMENT :

PRODUCTEUR DE DÉTAIL		**PRODUCTEUR EN GROS**	
Nom du producteur :		Nom du producteur :	
Ville, État :		Ville, État :	
Numéro de téléphone		Numéro de téléphone	
Numéro de licence :		Numéro de licence :	

SIGNATURE DU PRODUCTEUR :