# FORMULAIRE DE DEMANDE - ASSURANCE CYBER

Le présent formulaire de demande est destiné aux organisations dont le chiffre d'affaires consolidé du groupe est inférieur ou égal à 500 millions. Les candidats dont le chiffre d'affaires est supérieur à 500 millions ou qui exercent des activités dans des secteurs à haut risque doivent contacter AIG pour obtenir le formulaire approprié. Les secteurs suivants sont considérés comme à haut risque : Compagnies aériennes, Aviation, Établissements financiers, Hôpitaux et établissements/cabinet de santé, Cabinets d'avocats, Prestataires de Services Managés (MSP) et Prestataires de Services de Sécurité Managés (MSSP), Processeurs de paiement, et Entités publiques (y compris les municipalités) et Établissements scolaires (y compris les écoles primaires, secondaires et les universités).

*"**le Demandeur**" désigne individuellement et collectivement chaque personne ou entité demandant à être couverte par la présente assurance. Les informations fournies dans cette Demande seront utilisées pour déterminer l'étendue et les possibilités d'une offre d'assurance.*

*"**l'Assureur**" désigne la société d'assurance affiliée à American International Group, Inc. qui délivre la police au **Demandeur** sur la base de la présente Demande.*

| INFORMATIONS GÉNÉRALES | | |
|---|---|---|
| Nom complet du demandeur : | | |
| Le demandeur est : | Holding | Filiale |
| Page(s) Web du demandeur : | | |
| Nombre d'employés de demandeur : | | |
| Estimation du chiffre d'affaires annuel du demandeur : | | |

Sélectionnez la/les région(s) dans laquelle/lesquelles le Demandeur exerce ses activités. Le % total du chiffre d'affaires doit être égal à 100%.
(cocher toutes les cases correspondantes)

| | | | | | |
|---|---|---|---|---|---|
| Australie et Nouvelle-Zélande | % | Canada | % | États-Unis | % |
| Asie de l'Est et Pacifique | % | Europe (hors UK) | % | Asie centrale et Asie du Sud | % |
| Moyen-Orient et Afrique du Nord | % | Russie | % | Mexique, Amérique centrale et Caraïbes | % |
| Amérique du Sud | % | Royaume-Uni | % | Afrique du Sud | % |
| | | | | **Total :** | % |

| Veuillez renseigner les informations suivantes concernant le Responsable de la Sécurité des Systèmes d'Information (RSSI) du Demandeur, ou l'équivalent, qui est responsable du maintien de la posture de cybersécurité du Demandeur. | |
|---|---|
| Nom : | |
| Titre : | |
| E-mail : | |

*L'**Assureur** peut, mais n'y est pas obligé, (1) d'utiliser des données observables externes concernant le réseau informatique du **Demandeur**, et (2) de contacter le Responsable de la Sécurité des Systèmes d'Information du **Demandeur** (ou autre personne désignée ci-dessus) en lien avec une condition ou une circonstance que l'**Assureur** estime raisonnablement susceptible d'entraîner un sinistre futur couvert par la police demandée. L'**Assureur** peut continuer à observer et à rapporter, comme décrit ci-dessus, pendant la durée de toute police contenant la couverture délivrée au **Demandeur**.*

| **TRAITEMENT DES DONNÉES** | |
|---|---|
| Veuillez indiquer le volume de données de chaque catégorie que le Demandeur collecte, traite, stocke ou qui sont transférées dans son environnement, y compris les enregistrements collectés, traités ou stockés par d'autres pour le compte du Demandeur. | |
| Enregistrements uniques d'Informations Personnelles Identifiables (IPI) (y compris les IPI des employés) : | |
| Enregistrements uniques d'Informations de Santé Protégées (ISP) : | Non applicable |
| Nombre d'Informations de Paiement (PCI) uniques : | Non applicable |
| Nombre d'identifiants biométriques uniques : | Non applicable |

| SECTEUR D'ACTIVITÉ | | | | | |
|---|---|---|---|---|---|
| Sélectionnez le(s) secteur(s) d'activité dans le(s)quel(s) le Demandeur exerce. Le % total du chiffre d'affaires doit être égal à 100%. | | | | | |
| Experts-comptables | % | Professionnels, Scientifiques, and Consultants techniques | % | Information, Logiciels, and Technologie (hors traitement de paiements) | % |
| Agriculture, Foresterie, Mines, Pêche et Chasse | % | Jeux, y compris les casinos | % | Télémarketing | % |
| Avocats | % | Entités gouvernementales | % | Agence d'intérim, services de recrutement et gestion de paie | % |
| Agents de recouvrement | % | Santé et Aide sociale | % | Administrateurs tiers | % |
| BTP | % | Hôtels / Hébergement | % | Transport et Entreposage | % |
| Agences de crédit | % | Industrie manufacturière | % | Agences de voyage | % |
| Restauration | % | Entités liées aux médias | % | Commerce de gros | % |
| Enseignement (secteur lié) | % | Traitement de paiements | % | Services publics | % |
| Établissements financiers | % | Immobilier | % | Gestion des déchets, Services d'assainissement, Administration et Support | % |
| Services financiers (Autres que les établissements financiers) | % | Commerce de détail | % | Non listé (Veuillez préciser) | % |
| | | | | **Total :** | % |

| SECTION EXPOSITION | | |
|---|---|---|
| a) Le Demandeur utilise-t-il les Services de Domaine Active Directory de Microsoft ("ADDS"), que ce soit en local ("on-premises"), hébergé ou dans une configuration hybride ? Pour éviter toute ambiguïté : avec ADDS, nous NE FAISONS PAS référence à Azure Active Directory ("Azure AD") ou Microsoft Entra ID. | Oui | Non |
| b) La Société utilise-t-elle Microsoft Exchange, y compris dans un "déploiement hybride" ? | Oui | Non |
| c) La Société utilise-t-elle des logiciels non supportés (des logiciels pour lesquels l'éditeur ne fournit plus de correctifs de sécurité) ? | Oui | Non |

| SECTION CONTRÔLES | | |
|---|---|---|
| Veuillez indiquer les contrôles en place dans l'environnement du Demandeur. Pour cela, "environnement" désigne à la fois la partie interne et externalisée de l'environnement du Demandeur. Si une réponse ne correspond pas à 100% à la situation du Demandeur, veuillez sélectionner "Non" et fournir des informations supplémentaires sur les nuances si nécessaire, soit dans la zone de commentaires en page 7, soit dans un document séparé. | | |
| **1. Sauvegardes et capacités de reprise d'activité** | | |
| a) Un processus de création de sauvegardes régulières existe (même s'il n'est pas documenté et/ou ad hoc). | Oui | Non |
| b) La stratégie de sauvegarde inclut des sauvegardes régulières hors ligne (sur site ou hors site). | Oui | Non |
| c) Les sauvegardes sont isolées et séparées du domaine de production (c'est-à-dire des sauvegardes cloud protégées par MFA) ou elles sont immuables. | Oui | Non |
| d) Un plan de réponse aux incidents documenté est en place. | Oui | Non |

| **2. Authentification à distance – veuillez sélectionner une seule réponse -** | |
|---|---|
| a) L'accès à distance aux ressources de l'entreprise nécessite généralement uniquement un nom d'utilisateur et un mot de passe valides (authentification à un seul facteur). | |
| b) Le MFA est requis et appliqué pour tout accès à distance des employés au réseau d'entreprise, et toutes les exceptions à la politique sont documentées. | |
| c) Le MFA est requis et appliqué pour tout accès à distance (employés, fournisseurs et SaaS tiers), et toutes les exceptions à la politique sont documentées. | |
| d) L'accès à distance aux ressources de l'entreprise n'est pas du tout fourni. | |

| 3. Politiques de mots de passe | | | |
|---|---|---|---|
| a) | Un gestionnaire de mots de passe est fourni à tous les employés. | Oui | Non |
| b) | Une politique interdisant la réutilisation des mots de passe est en vigueur (utilisation de mots de passe uniques pour les applications de l'environnement). | Oui | Non |
| c) | Les comptes de service (comptes utilisés par des machines - et non des personnes - pour exécuter des applications et d'autres processus) ont des mots de passe d'au moins 25 caractères. | Oui | Non |

| 4. Surveillance et réponse | | | | |
|---|---|---|---|---|
| a) | Un outil de "Surveillance des Événements et des Informations de Sécurité" (SIEM) est en place. | | Oui | Non |
| b) | L'environnement est surveillé pour détecter les transferts de données anormaux et potentiellement suspects. | | Oui | Non |
| c) | Un "Centre des Opérations de Sécurité" ou SOC est en place pour surveiller les incidents de sécurité, en interne et/ou assuré par un MSSP (Prestataire de Services de Sécurité Managés) | Oui, 24h/24 et 7j/7 | Oui, mais pas 24h/24 et 7j/7 | Non |
| d) | Un plan de réponse aux incidents documenté, axé spécifiquement sur la gestion des cyber incidents, est en place. | | Oui | Non |

| 5. Défense conte l'hameçonnage : facteur humain | | | |
|---|---|---|---|
| a) | Une formation de sensibilisation à la sécurité, incluant la formation à la sensibilisation à l'hameçonnage, est dispensée aux employés au moins une fois par an. | Oui | Non |
| b) | Des simulations d'attaques par hameçonnage sont utilisées pour tester la sensibilisation à la cybersécurité des employés au moins une fois par an. | Oui | Non |
| c) | Un processus documenté permet de signaler les e-mails suspects à une équipe de sécurité (interne) pour investigation. | Oui | Non |

| 6. Défense conte l'hameçonnage : aspects techniques | | | |
|---|---|---|---|
| a) | Les e-mails provenant de l'extérieur de l'organisation sont "marqués" ou identifiés comme tels. | Oui | Non |
| b) | Une solution de filtrage des e-mails est en place, bloquant les pièces jointes malveillantes connues et les types de fichiers suspects, y compris les exécutables. | Oui | Non |
| c) | Une solution de filtrage Web est en place. | Oui | Non |
| d) | La solution de filtrage Web est efficace sur tous les actifs de l'organisation, même si l'actif n'est pas sur le réseau de l'organisation (par exemple, les actifs sont configurés pour utiliser des filtres Web basés sur le cloud ou nécessitent une connexion VPN pour naviguer sur Internet). | Oui | Non |

**Zone de commentaires pour les questions précédentes**

| |
|---|
| |

| **7. Outils de sécurité des terminaux** | | |
|---|---|---|
| a) La solution de sécurité des terminaux inclut un antivirus avec des capacités heuristiques et/ou des outils avec des capacités de détection comportementale et d'atténuation des exploits. | Oui | Non |
| b) Un outil de Détection et Réponse sur les Terminaux (EDR) est en place, qui effectue les actions suivantes : surveille les indicateurs de menace ; identifie les modèles correspondant à des menaces connues ; répond automatiquement en supprimant ou en contenant les menaces ; alerte le personnel de sécurité des incidents ; fournit des capacités forensiques et d'analyse permettant aux analystes d'effectuer des activités de chasse aux menaces. | Oui | Non |

| **8. Périmètre des Outils de Sécurité des Terminaux** | | |
|---|---|---|
| a) La solution de sécurité des terminaux mentionnée dans la question précédente est déployée sur toutes les stations de travail et ordinateurs portables. | Oui | Non |
| b) La solution de sécurité des terminaux mentionnée dans la question précédente est déployée sur tous les serveurs. | Oui | Non |
| c) Pour la solution de sécurité des terminaux mentionnée dans la question précédente, les mises à jour automatiques sont activées. | Oui | Non |
| d) La solution de sécurité des terminaux mentionnée dans la question précédente est configurée pour bloquer (et non pas seulement notifier) les processus/fichiers suspectés malveillants. | Oui | Non |

| **9. Mise à jour corrective (Patching)** | | | |
|---|---|---|---|
| a) Quelle est la capacité à déployer les correctifs de priorité la plus haute en dehors des processus de mise à jour corrective périodiques réguliers ? (par exemple, en cas d'exploitation active d'une vulnérabilité logicielle pour laquelle un correctif hors cycle est disponible) ? | 0-3 jours | 3-7 jours | >7 jours |
| b) Des analyses régulières de vulnérabilités des environnements exposés vers l'extérieur sont-elles réalisées ? | | Oui | Non |

**Zone de commentaires pour les questions précédentes**

| |
|---|
| |

| **10. Segmentation et protection** | | | |
|---|---|---|---|
| a) Des règles de pare-feu réseau et/ou hôte sont implémentées pour empêcher l'utilisation du RDP (Remote Desktop Protocol) exposé vers l'extérieur pour se connecter aux postes de travail. | | Oui | Non |
| b) Un inventaire de tous les comptes de service (comptes utilisés par des machines -- et non des personnes - pour exécuter des applications et d'autres processus) existe-t-il ? | Oui | Non | Nous n'avons pas de comptes de service |
| c) Des pares-feux réseau ont été déployés sur tous les sites du Demandeur. | | | |

| **11. Protection des données** | | |
|---|---|---|
| a) Les données sont chiffrées sur les appareils des utilisateurs finaux pour les protéger en cas de perte d'appareil. Des exemples de mise en œuvre incluent Windows Bitlocker, Apple FileVault et Linux dm-crypt. | Oui | Non |

**Zone de commentaires pour les questions précédentes**

| |
|---|
| |

| SECTION FOURNISSEURS DE SERVICES EXTERNES | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Veuillez indiquer le nom du/des fournisseur(s) tiers que vous utilisez pour chacune des catégories suivantes. Si le Demandeur n'utilise pas de fournisseur tiers et utilise uniquement des capacités/services internes ou si la catégorie n'est pas applicable aux activités du Demandeur, cochez la case N/A pour cette catégorie. Si d'autres fournisseurs tiers importants pour les activités du Demandeur ne sont pas listés, utilisez la section "Autre(s) à préciser". | | | | | | | | | | | | |
| **Services d'hébergement** | | **Services de messagerie et associés** | | **Logiciel de relation client/CRM** | | **Gestion des RH** | | **Services de e-commerce et de paiement** | | **Prestataires de services de sécurité** | | **Fournisseurs de contrôle industriel** |
| | N/A | | N/A | | N/A | | N/A | | N/A | | N/A | | N/A |
| | Accenture | | Amazon AWS SES | | Aptean | | ADP | | Adyen B.V | | Accenture | | ABB |
| | Akamai | | AppRiver, LLC | | Astute | | Avature Recruiting | | Amazon AWS | | Akamai | | Bosch |
| | Amazon AWS | | Barracuda Networks | | Atos | | Ceridian | | Apple | | Atos | | Emerson |
| | Atos | | CyrenCorporation | | Deltek | | Cornerstone | | Atos | | Carbon Black | | GE |
| | AT&T | | GoDaddy | | eGain | | Fujitsu | | BlueSnap | | Cisco | | Honeywell |
| | CloudFlare | | Google | | Gainsight | | HCL Technologies | | CCBill | | CloudFlare | | Metso |
| | Dell | | Intuit Mailchimp | | Google | | iCIMS | | EverCommerce | | Comodo Group | | Mitsubishi Electric |
| | Equinix | | MailChannels | | Infor | | IBM | | Fidelity National Information Services | | CrowdStrike | | Rockwell Automation |
| | Fujitsu | | McAfee, Inc | | Medallia Inc | | Jobvite | | Fujitsu | | Dell | | Rolls Royce |
| | F5 Networks | | Microsoft | | Microsoft | | Kronos | | Ingenico | | DigiCert | | Schneider |
| | Gandi SAS | | Mimecast | | Oracle | | NICE Systems | | Klarna AB | | Fujitsu | | Siemens |
| | Google | | Proofpoint | | Sage Group | | Oracle | | NCR Corporation | | GMO GlobalSign | | Toshiba |
| | HCL Technologies | | Rackspace | | Salesforce.com | | PeopleAdmin | | PayPal | | HCL Technologies | | Yokogawa |
| | Hewlett Packard | | SendGrid, Inc | | SAP | | PeopleFluent | | Recurly | | Hewlett Packard | | |
| | IBM | | Symantec | | Veeva Systems | | SAP | | Square | | IBM | | |
| | Microsoft | | United Internet AG | | Zoho Corporation | | WorkDay | | Stripe | | Let's Encrypt | | |
| | Newfold Digital | | | | | | Xactly Corporation | | VeriFone Systems | | McAfee | | |
| | OVH SAS | | | | | | | | | | Microsoft | | |
| | Rackspace | | | | | | | | | | Okta | | |
| | Siemens | | | | | | | | | | Palo Alto | | |
| | Telefonica | | | | | | | | | | Sentinel One | | |
| | United Internet AG | | | | | | | | | | Siemens | | |
| | Verizon | | | | | | | | | | Symantec | | |
| | Wipro | | | | | | | | | | Tenable Network | | |

| Autre(s) à préciser | Autre(s) à préciser | Autre(s) à préciser | Autre(s) à préciser | Autre(s) à préciser | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | Sentinel One | Autre(s) à préciser |
| | | | | | | Siemens | |
| | | | | | | Symantec | |
| | | | | | | Tenable Network | |
| | | | | | **Autre(s) à préciser** | | |
| | | | | | | | |

| SECTION ANTÉCÉDENTS DE SINISTRES, CIRCONSTANCES ET GARANTIES | | |
|---|---|---|
| 1. Le Demandeur a-t-il connu l'un des incidents suivants au cours des 5 dernières années ayant eu un impact sur ses opérations commerciales ? | | |
| a) Ransomware | Oui | Non |
| b) Violations significatives de données/vie privée | Oui | Non |
| c) Autres incidents de sécurité ayant eu un impact significatif | Oui | Non |

* Si oui à l'une des questions ci-dessus, veuillez fournir, par incident, les informations suivantes :
- Résumé de l'incident et description de la cause racine.
- Les améliorations apportées à l'environnement pour prévenir une attaque future.
- Si un rapport forensique est disponible, veuillez-nous en envoyer une copie.
- Une estimation de la perte totale subie, incluant mais sans s'y limiter, les honoraires forensiques IT, juridiques, de relations publiques, les coûts de redressement, d'interruption d'activité et de responsabilité, etc.)

| | | |
|---|---|---|
| 2. Le Demandeur a-t-il un établissement, une filiale, une participation ou une coentreprise et/ou le Demandeur exerce-t-il des activités (avec des partenaires) dans des pays soumis à des sanctions imposées par les Nations Unies, les États-Unis d'Amérique, l'Union Européenne, ou le pays dans lequel réside le bureau AIG gestionnaire ? | Oui | Non |

| DECLARATION DE NON-SINISTRE | |
|---|---|
| Le Demandeur a-t-il connaissance d'une situation ou circonstance telle que, sans s'y limiter, toute occurrence, sinistre ou perte liée à une défaillance de la sécurité des systèmes informatiques du Demandeur, ou quelqu'un a-t-il intenté un procès ou déposé une réclamation contre le Demandeur concernant une violation ou une ingérence dans les droits à la vie privée, une divulgation illicite d'Informations Confidentielles qui pourrait entraîner une réclamation contre le Demandeur relative aux questions liées à l'Assurance Demandée ? | |
| Oui | |
| Non | |
| Non applicable (l'Assurance Demandée est le renouvellement de la couverture avec l'Assureur) | |

**Il est convenu qu'en ce qui concerne ce qui précède, si de telles circonstances, sinistres, pertes ou connaissances existent, toute perte ou sinistre découlant de ces occurrences, sinistres, pertes ou connaissances sera exclue de la couverture proposée.**

| SECTION SIGNATURE |
|---|
| Le soussigné, dûment autorisé à représenter le Demandeur, reconnaît par la présente qu'une enquête raisonnable a été menée pour obtenir des réponses qui sont, à sa connaissance et à sa conviction, vraies, correctes et complètes.<br>L'officier autorisé soussigné du Demandeur reconnaît par la présente qu'il a pris connaissance que la Limite de Responsabilité stipulée dans cette police sera réduite, et peut être entièrement épuisée, par les frais de défense juridique et, en pareil cas, l'Assureur ne sera pas responsable des frais de défense juridique ou du montant de tout jugement ou règlement dans la mesure où ceux-ci excèdent la Limite de Responsabilité de cette police.<br>L'officier autorisé soussigné du Demandeur reconnaît en outre par la présente qu'il a pris connaissance que les frais de défense juridique engagés seront imputés sur le montant de la franchise.<br>L'officier autorisé soussigné du Demandeur reconnaît en outre par la présente avoir lu, compris et accepté les avis finaux figurant sur la dernière page de ce document. |

**Signé**
**(Représentant dûment autorisé, pour et au nom du Demandeur)**

## DOCUMENTS ET INFORMATIONS ADDITIONNELS INCORPORÉS PAR RÉFÉRENCE

TOUTES DÉCLARATIONS ÉCRITES, DOCUMENTS OU MATÉRIAUX FOURNIS À L'ASSUREUR CONJOINTEMENT AVEC CETTE DEMANDE, INDÉPENDAMMENT DU FAIT QUE CES DOCUMENTS SOIENT ANNEXÉS À LA POLICE, SONT INCORPORÉS PAR RÉFÉRENCE DANS CETTE DEMANDE ET EN DEVIENNENT PARTIE INTÉGRANTE, Y COMPRIS, SANS LIMITATION, TOUTES DEMANDES OU QUESTIONNAIRES COMPLÉMENTAIRES.

TOUTE ÉVALUATION DE SÉCURITÉ, TOUTES DÉCLARATIONS FAITES CONCERNANT UNE ÉVALUATION DE SÉCURITÉ, ET TOUTES INFORMATIONS CONTENUES DANS OU FOURNIES PAR LE DEMANDEUR CONCERNANT UNE ÉVALUATION DE SÉCURITÉ, INDÉPENDAMMENT DU FAIT QUE CES DOCUMENTS, INFORMATIONS OU DÉCLARATIONS SOIENT ANNEXÉS À LA POLICE, SONT INCORPORÉS PAR RÉFÉRENCE DANS CETTE DEMANDE ET EN DEVIENNENT PARTIE INTÉGRANTE.

**AVIS JURIDIQUES ET SIGNATURES**

AVANT DE SIGNER CETTE DEMANDE, LISEZ ATTENTIVEMENT CES AVIS ET DISCUTEZ-EN AVEC VOTRE COURTIER SI VOUS AVEZ DES QUESTIONS.
AUX FINS DE CETTE DEMANDE, LE REPRÉSENTANT DÛMENT AUTORISÉ SOUSSIGNÉ DE TOUTES LES PERSONNES ET ENTITÉS PROPOSÉES POUR CETTE ASSURANCE DÉCLARE QUE, À SA CONNAISSANCE ET SA CONVICTION, APRÈS ENQUÊTE RAISONNABLE, LES DÉCLARATIONS DANS CETTE DEMANDE, ET DANS TOUTES LES PIÈCES JOINTES, SONT VRAIES ET COMPLÈTES.
LE REPRÉSENTANT DÛMENT AUTORISÉ SOUSSIGNÉ CONVIENT QUE SI LES DÉCLARATIONS ET INFORMATIONS FOURNIES DANS CETTE DEMANDE OU INCORPORÉES PAR RÉFÉRENCE CHANGENT ENTRE LA DATE DE CETTE DEMANDE ET LA DATE D'EFFET DE L'ASSURANCE, IL (LE SOUSSIGNÉ) INFORMERA IMMÉDIATEMENT L'ASSUREUR DE CES CHANGEMENTS AFIN QUE LES INFORMATIONS SOIENT EXACTES À LA DATE D'EFFET DE L'ASSURANCE, ET L'ASSUREUR POURRA RETIRER OU MODIFIER TOUT DEVIS ET/OU AUTORISATION OU ACCORD EN COURS POUR GARANTIR L'ASSURANCE.

LA SIGNATURE DE CETTE DEMANDE N'ENGAGE PAS LE DEMANDEUR OU L'ASSUREUR À CONCLURE L'ASSURANCE, MAIS IL EST CONVENU QUE CETTE DEMANDE ET TOUTE INFORMATION INCORPORÉE PAR RÉFÉRENCE SERONT LA BASE DU CONTRAT SI UNE POLICE EST DÉLIVRÉE ET SONT INCORPORÉES À LA POLICE ET EN FONT PARTIE INTÉGRANTE.

SI L'ASSUREUR DÉLIVRE UNE POLICE, LE DEMANDEUR ACCEPTE QUE CETTE POLICE EST DÉLIVRÉE EN SE FONDANT SUR LA VÉRACITÉ DES DÉCLARATIONS ET REPRÉSENTATIONS DANS CETTE DEMANDE OU INCORPORÉES PAR RÉFÉRENCE. TOUTE DÉCLARATION INEXACTE, OMISSION, DISSIMULATION OU DÉCLARATION ERRONÉE D'UN FAIT MATÉRIEL, DANS CETTE DEMANDE, INCORPORÉE PAR RÉFÉRENCE OU AUTREMENT, CONSTITUERA UN MOTIF DE RÉSILATION DE TOUTE POLICE DÉLIVRÉE.

AVIS AUX DEMANDEURS : TOUTE PERSONNE QUI, SCIEMMENT ET AVEC L'INTENTION DE FRAUDER TOUTE COMPAGNIE D'ASSURANCE OU TOUTE AUTRE PERSONNE, DÉPOSE UNE DEMANDE D'ASSURANCE OU UNE DÉCLARATION DE SINISTRE CONTENANT TOUTE INFORMATION MATÉRIELLEMENT FAUSSE OU, DISSIMULE, DANS LE BUT D'INDURE EN ERREUR, DES INFORMATIONS CONCERNANT TOUT FAIT MATÉRIEL, COMMET UN ACTE FRAUDULEUX, QUI EST UN CRIME ET PEUT EXPOSER CETTE PERSONNE À DES POURSUITES PÉNALES ET CIVILES.

LE DEMANDEUR ACCEPTE QUE LES INFORMATIONS DANS CETTE DEMANDE PUISSENT ÊTRE UTILISÉES POUR FOURNIR OU AMÉLIORER LES PRODUITS, SERVICES OU PROGRAMMES DE GESTION DES RISQUES.

Si vous avez des questions sur des faits que vous savez déjà connus de l'assureur, vous devez répondre de la manière la plus complète possible. Si vous n'avez pas (entièrement) respecté votre obligation d'information, cela peut entraîner une restriction voire une perte du droit aux prestations. Si vous avez agi intentionnellement pour tromper l'assureur ou si l'assureur n'aurait pas conclu le contrat d'assurance en connaissant la véritable situation, l'assureur a également le droit de résilier le contrat d'assurance.

Si la loi le permet, les principes suivants s'appliquent également à l'obligation de fournir des informations pour cette demande d'assurance :

- Une question sans réponse ou ouverte est réputée avoir reçu une réponse négative ;
- La 'question finale' doit être répondue intégralement. La 'question finale' est réputée avoir été répondue de manière incomplète si des faits et circonstances ont été omis ou inexacts de la part du demandeur, par exemple sur la base des autres questions posées dans le formulaire de demande et/ou de la nature de l'assurance demandée par rapport à ce qui n'a pas été déclaré ou a été inexact, il doit avoir été raisonnablement compris que ceux-ci pourraient être importants pour l'évaluation du risque proposé à l'assurance.