La traduction suivante est fournie à des fins d'information uniquement. En cas de divergence, d'incohérence ou de conflit entre cette traduction et la version anglaise (en particulier en cas de retard de traduction), la version anglaise aura préséance.

POLITIQUE DE SÉCURITÉ DES PRESTATAIRES

Dernière mise à jour : 28 janvier 2022

1. PORTÉE ET DÉFINITIONS.

1.1 Politique de sécurité. Le Prestataire se conformera à tous égards aux exigences d'Amazon en matière de sécurité de l'information énoncées dans la présente politique (la « **Politique de sécurité** »). La présente Politique de sécurité s'applique à l'exécution par le Prestataire en vertu de l'Accord et à tous les accès, collectes, utilisations, stockages, transmissions, divulgations, destructions ou effacements des Informations Amazon, ainsi qu'aux incidents de sécurité relatifs aux Informations Amazon. La présente Politique de sécurité ne limite aucune des autres obligations du Prestataire, y compris en vertu d'autres accords avec Amazon ou de toute autre loi qui s'applique au Prestataire, à l'exécution par le Prestataire en vertu d'autres accords avec Amazon, aux Informations Amazon ou à la Finalité autorisée. Si la présente Politique de sécurité est en conflit avec tout accord de confidentialité entre les parties, ou tout autre accord applicable aux parties, le Prestataire informera rapidement Amazon du conflit et se conformera aux exigences qui sont plus protectrices des Informations Amazon, à moins que les exigences moins protectrices ne soient expressément énoncées comme dépassant les exigences plus protectrices (qui peuvent être énoncées par Amazon). Amazon peut modifier la présente Politique de sécurité de temps à autre, à sa discrétion exclusive, étant entendu que, si ces modifications ne sont pas commercialement raisonnables, Amazon agréera les frais supplémentaires appropriés susceptibles de lui être demandés.

1.2 Définitions.

1.2.1 « **Agréger** » signifie combiner ou stocker des Informations Amazon avec des données ou des informations du Prestataire ou de tout tiers.

1.2.2 « **Accord** » signifie tout accord qui fait référence à la présente Politique de sécurité.

1.2.3 « **Amazon** » désigne Amazon.com, Inc. et ses sociétés affiliées.

1.2.4 « **Anonymiser** » signifie utiliser, collecter, stocker, transmettre ou transformer toute donnée ou information (y compris les Informations Amazon) d'une manière ou d'une forme qui ne permet pas d'identifier et n'est pas autrement attribuable à Amazon, ou à tout utilisateur, identifiant d'appareil, source, produit, service, contexte ou marque de ceux-ci.

1.2.5 « **Informations Amazon** » signifie, individuellement et collectivement : (a) toutes les Informations confidentielles d'Amazon (telles que définies dans un accord de confidentialité ou tout autre accord entre les parties) ; (b) tous les autres données, dossiers, fichiers, contenu, ou informations, sous n'importe quelle forme ou format, acquis, accédés, collectés, reçus, stockés, ou maintenus par le Prestataire ou ses sociétés affiliées, de la part de ou au nom d'Amazon, ou autrement en lien avec la présente Politique de sécurité ou les services, ou l'exécution ou l'exercice par les parties des droits en vertu de l'Accord ou en relation avec celui-ci ; et (c) les informations dérivées des points (a) ou (b), même si elles sont anonymisées.

1.2.6 « Prestataire » désigne chaque Prestataire, Fournisseur ou Sous-traitant défini dans un Accord et tout autre prestataire soumis à un Accord.

1.3 Finalité autorisée. Le Prestataire peut accéder, collecter, utiliser, stocker et transmettre uniquement les Informations Amazon expressément autorisées en vertu de l'Accord et uniquement aux fins de fournir les produits ou services en vertu de l'Accord, conformément aux licences (le cas échéant) accordées en vertu de la présente Politique de sécurité (la « **Finalité autorisée** »). Sauf autorisation expresse en vertu de l'Accord, le Prestataire

n'accédera pas, ne collectera pas, n'utilisera pas, ne stockera pas ou ne transmettra pas d'Informations Amazon et ne regroupera pas les Informations Amazon, même si elles sont anonymisées. À l'exception du consentement écrit exprès préalable d'Amazon, le Prestataire s'abstiendra (a) de transférer, louer, troquer, échanger, vendre, prêter ou autrement de distribuer ou de mettre à la disposition de tout tiers, toute Information Amazon ou (b) d'agréger les Informations Amazon avec toute autre information ou donnée, même si elles sont anonymisées.

2. POLITIQUE DE SÉCURITÉ AMAZON.

2.1 Exigences de sécurité de base. Le Prestataire, conformément aux meilleures normes actuelles du secteur et aux autres exigences spécifiées par Amazon en fonction de la classification et de la sensibilité des Informations Amazon, maintiendra des garanties physiques, administratives et techniques et d'autres mesures de sécurité pour (a) maintenir la sécurité et la confidentialité des Informations Amazon consultées, collectées, utilisées, stockées, ou transmises par le Prestataire, et (b) protéger ces informations contre les menaces ou les dangers connus ou raisonnablement anticipés pour leur sécurité et leur intégrité, de perte accidentelle, d'altération, et de divulgation et toutes les autres formes illégales de traitement. Sans limitation, le Prestataire se conformera aux exigences suivantes pour tous les systèmes que le Prestataire utilise pour traiter les Informations Amazon ou qui ont accès aux Informations Amazon (« **Systèmes d'information Amazon** ») :

2.1.1 Sécurité réseau. Le Prestataire protégera tous les Systèmes d'information Amazon en limitant l'accès non autorisé au réseau, en particulier depuis l'Internet externe. Le Prestataire installera et maintiendra une solution de sécurité réseau efficace, telle qu'un pare-feu, pour protéger les Informations Amazon à tout moment.

2.1.2 Mises à jour. Comme indiqué dans la publication spéciale (SP) 800-40, Révision 3 de l'Institut national des normes et de la technologie (National Institute of Standards and Technology, « NIST »), le Prestataire tiendra les Systèmes d'information Amazon à jour avec les dernières mises à niveau, mises à jour, corrections de bogues et nouvelles versions, ainsi qu'avec toute autre modification nécessaire pour assurer la sécurité des Informations Amazon.

2.1.3 Anti-malware. Le Prestataire utilisera à tout moment un logiciel anti-malware ou un contrôle de sécurité équivalent pour atténuer le risque de compromission et de propagation des logiciels malveillants. S'il est utilisé, le Prestataire tiendra à jour les logiciels anti-malware.

2.1.4 Chiffrement. Le Prestataire chiffrera les données au repos et les données envoyées sur des réseaux ouverts conformément aux meilleures pratiques du secteur.

2.1.5 Test. Le Prestataire testera régulièrement ses systèmes et processus de sécurité pour s'assurer qu'ils répondent aux exigences de la présente Politique de sécurité ou à la dernière politique de sécurité convenue par le Prestataire et Amazon. Dans la mesure où des modifications sont apportées à la Politique de sécurité conformément à la Section 1.1, ces modifications prendront effet aux fins de la présente section seulement lors d'un accord entre le Prestataire et Amazon (un e-mail suffit).

2.1.6 Contrôles d'accès. Le Prestataire sécurisera les Informations Amazon, y compris en se conformant aux exigences suivantes :

2.1.6.1 Le Prestataire attribuera un identifiant unique à chaque personne ayant un accès informatique aux Informations Amazon ou aux Systèmes d'information Amazon.

2.1.6.2 Le Prestataire limitera l'accès aux Informations Amazon aux seules personnes ayant besoin d'en avoir connaissance pour une Finalité autorisée.

2.1.6.3 Le Prestataire examinera régulièrement la liste des personnes et des services ayant accès aux Informations Amazon, et supprimera les comptes qui n'ont plus besoin d'accéder aux Systèmes d'information Amazon. Cet examen doit être effectué au moins une fois tous les 90 jours.

2.1.6.4 Le Prestataire n'utilisera pas les valeurs par défaut fournies par le fabricant pour les mots de passe système et autres paramètres de sécurité sur les Systèmes d'information Amazon. Le Prestataire mandatera et veillera à l'utilisation de « mots de passe forts » imposés par le système conformément aux meilleures pratiques décrites dans NIST SP 800-63B sur tous les Systèmes

d'information Amazon. Le Prestataire exigera que tous les mots de passe et identifiants d'accès soient tenus confidentiels et ne soient pas partagés entre le personnel.

2.1.6.5 Le Prestataire maintiendra et appliquera le verrouillage de compte en désactivant les comptes ayant accès aux Informations Amazon ou aux Systèmes d'information Amazon lorsqu'un compte dépasse plus de dix (10) tentatives consécutives de mot de passe incorrect.

2.1.6.6 Sauf autorisation expresse écrite d'Amazon, le Prestataire séparera physiquement ou logiquement les Informations Amazon à tout moment (y compris lors du stockage, du traitement ou de la transmission), des informations du Prestataire et de tout tiers.

2.1.6.7 Si des contrôles d'accès physique supplémentaires sont demandés par écrit par Amazon, le Prestataire mettra en œuvre et utilisera ces mesures de contrôle d'accès physique sécurisé.

2.1.6.8 Le Prestataire fournira à Amazon, sur demande raisonnable d'Amazon, (a) des données de journal sur toute utilisation (autorisée et non autorisée) des comptes ou informations d'identification d'Amazon fournies au Prestataire pour une Finalité autorisée (par ex., informations d'identification de compte de réseau social), et (b) des données de journal détaillées sur toute usurpation d'identité ou tentative d'usurpation d'identité du personnel d'Amazon ou du Prestataire qui a accès aux Informations Amazon.

2.1.6.9 Le Prestataire examinera régulièrement les journaux d'accès à la recherche de signes de comportement malveillant ou d'accès non autorisé.

2.1.7 Politique du prestataire. Le Prestataire maintiendra et appliquera une politique de sécurité des informations et du réseau pour les employés, sous-traitants, représentants et prestataires qui répondent aux normes énoncées dans la présente Politique de sécurité, y compris les méthodes pour détecter et consigner les violations de la politique. Sur demande d'Amazon, le Prestataire fournira à Amazon des informations sur les violations de la politique de sécurité des informations et du réseau du Prestataire si le Prestataire ou Amazon ont une suspicion raisonnable que cela puisse constituer un Incident de sécurité (défini ci-dessous).

2.1.8 Sous-traitance. Le Prestataire ne sous-traitera ni ne déléguera aucune de ses obligations en vertu de la présente Politique de sécurité à des sous-traitants ou délégués (collectivement, « **Sous-traitants** ») sans le consentement écrit préalable d'Amazon. Nonobstant l'existence ou les conditions de tout contrat de sous-traitance ou toute délégation, le Prestataire demeurera responsable de l'exécution complète de ses obligations en vertu de la présente Politique de sécurité. Les conditions générales de la présente Politique de sécurité seront contraignantes pour les Sous-traitants et le Personnel du prestataire. Le Prestataire (a) veillera à ce que ses Sous-traitants et son personnel respectent la présente Politique de sécurité, et (b) sera responsable de tous les actes, omissions, négligences et fautes professionnelles des Sous-traitants et du Personnel du prestataire.

2.1.9 Accès à distance. Le Prestataire s'assurera que tout accès aux Systèmes d'information Amazon nécessite une authentification multi-facteurs (par exemple, nécessite au moins deux facteurs distincts pour identifier les utilisateurs).

2.1.10 Accès « en masse ». Aux fins de la présente section, l'accès « en masse » signifie le fait d'accéder aux données au moyen d'une requête de base de données, d'une génération de rapports ou de tout autre transfert de masse de données. Sauf autorisation expresse écrite d'Amazon, le Prestataire n'accédera pas et n'autorisera pas l'accès aux Informations Amazon « en masse », que les Informations Amazon soient dans une base de données contrôlée par le Prestataire ou Amazon ou stockées de toute autre manière, y compris le stockage dans des archives basées sur des fichiers (par exemple, des fichiers plats), etc. Plus précisément, cette section interdit tout accès aux Informations Amazon, à l'exception de l'accès aux dossiers individuels nécessaires pour la Finalité autorisée. Le Prestataire conservera les données détaillées des journaux concernant l'accès « en masse » tenté ou réussi aux Informations Amazon et fournira des rapports à partir de ces journaux dans le cadre des obligations du Prestataire en vertu de la section 2.5 (Examen de sécurité). Si Amazon fournit au Prestataire une autorisation écrite pour l'accès en masse aux Informations Amazon, le Prestataire (a) limitera cet accès uniquement aux employés spécifiés ayant besoin de les connaître et (b) utilisera des outils qui limitent l'accès et nécessitent une autorisation explicite et l'enregistrement de tous les accès.

2.1.11 Personnel du prestataire. Amazon peut imposer des conditions à l'accès du Personnel du prestataire aux Informations Amazon quant à l'exécution et à la livraison à Amazon d'accords individuels de non-divulgation, dont la forme est spécifiée par Amazon. Le Personnel du prestataire signera l'accord de non-divulgation individuel si Amazon l'exige. Le Prestataire obtiendra et livrera à Amazon les accords de non-divulgation individuels signés par le Personnel du prestataire qui aura accès aux Informations Amazon (avant d'accorder l'accès ou de fournir des informations au Personnel du prestataire). Le Prestataire tiendra également à jour une liste de tous les membres du Personnel du prestataire qui ont accédé aux Informations Amazon sur les Systèmes d'information Amazon ou qui les ont reçues, et fournira rapidement cette liste à Amazon sur demande. Pour tout membre du Personnel du prestataire qui (a) n'a plus besoin d'accéder aux Informations Amazon ou (b) n'est plus admissible en tant que membre du Personnel du prestataire (par ex., la personne quitte l'emploi du Prestataire), le Prestataire mettra immédiatement (dans un délai maximum de 24 heures) fin à l'accès aux Informations Amazon et aux Systèmes d'information Amazon. Si un tel personnel est autorisé à accéder aux Informations Amazon sur les Systèmes d'information Amazon, le Prestataire en informera également Amazon dans les 24 heures.

2.2 Accès à l'extranet Amazon et aux Portails des prestataires. Amazon peut accorder au Prestataire l'accès aux Informations Amazon via des portails Web ou d'autres sites Web non publics ou des services extranet sur le site Web ou le système d'Amazon ou d'un tiers (chacun, un « **Extranet** ») pour la Finalité autorisée. Si Amazon autorise le Prestataire à accéder à toute Information Amazon à l'aide d'un Extranet, le Prestataire doit se conformer aux exigences suivantes :

2.2.1 Finalité autorisée. Le Prestataire et le Personnel du prestataire accéderont à l'Extranet et auront accès à, collecteront, utiliseront, afficheront, récupéreront, téléchargeront ou stockeront les Informations Amazon depuis l'Extranet uniquement aux fins de la Finalité autorisée.

2.2.2 Comptes. Le Prestataire s'assurera que le Personnel du prestataire utilise uniquement le ou les compte(s) Extranet Amazon désignés pour chaque personne et exigera du Personnel du prestataire qu'il préserve la confidentialité de ses identifiants d'accès.

2.2.3 Systèmes. Le Prestataire n'accédera à l'Extranet que par le biais de systèmes informatiques ou de traitement ou d'applications exécutant des systèmes d'exploitation gérés par le Prestataire et qui comprennent : (a) des pare-feu de réseau système conformément à la section 2.1.1 (Sécurité du réseau) ; (b) une gestion centralisée des correctifs conformément à la section 2.1.2 (Mises à jour) ; (c) un logiciel anti-malware approprié au système d'exploitation conformément à la section 2.1.3 (Anti-malware) et (d) un disque complet de chiffrement pour les appareils portables.

2.2.4 Restrictions. Sauf approbation écrite préalable d'Amazon, le Prestataire s'abstiendra de télécharger, de dupliquer ou de stocker de manière permanente des Informations Amazon à partir d'un Extranet sur tout support, y compris les machines, appareils ou serveurs.

2.2.5 Résiliation de compte. Le Prestataire résiliera le compte d'Amazon, et informera Amazon au plus tard 24 heures après, de tout membre du Personnel du prestataire autorisé à accéder à l'Extranet qui : (a) n'a plus besoin d'accéder aux Informations Amazon ou (b) n'est plus qualifié en tant que membre du Personnel du prestataire (par exemple, le personnel met fin à son emploi avec le Prestataire).

2.2.6 Systèmes tiers.

2.2.6.1 Le Prestataire transmettra un préavis à Amazon et obtiendra l'approbation écrite préalable d'Amazon avant d'utiliser tout système tiers qui stocke ou peut autrement avoir accès aux Informations Amazon, sauf (a) si les données sont chiffrées conformément à la présente Politique de sécurité, et (b) si le système tiers n'a pas accès à la clé de déchiffrement ou aux versions non chiffrées des données en texte clair. Amazon se réserve le droit d'exiger un examen de sécurité Amazon (conformément à la section 2.5 (Examen de sécurité)) du système tiers avant de donner son approbation.

2.2.6.2 Si le Prestataire utilise des systèmes tiers qui stockent des Informations Amazon non chiffrées ou qui peuvent autrement accéder à des Informations Amazon non chiffrées, le Prestataire effectuera un examen de sécurité des systèmes tiers et de leurs contrôles de sécurité et fournira à Amazon des rapports périodiques sur les contrôles de sécurité du système tiers dans le format

demandé par Amazon (par ex., SAS 70 ou son rapport successeur, ou autre rapport reconnu approuvé par le secteur).

2.3 Conservation et destruction des données.

2.3.1 Conservation. Le Prestataire conservera les Informations Amazon uniquement aux fins de la Finalité autorisée, et aussi longtemps que nécessaire pour celle-ci.

2.3.2 Retour ou effacement. À la demande d'Amazon, le Prestataire retournera rapidement (mais pas plus de 72 heures) à Amazon et supprimera de manière permanente et sécurisée toutes les Informations Amazon conformément à l'avis d'Amazon exigeant un retour ou un effacement. Le Prestataire supprimera également de manière permanente et sécurisée toutes les instances en cours (en ligne ou accessibles par le réseau) des Informations Amazon dans les 30 jours suivant la réalisation de la Finalité autorisée ou la résiliation ou l'expiration de la présente Politique de sécurité. Si Amazon le demande, le Prestataire certifiera par écrit que toutes les Informations Amazon ont été détruites. Pour plus de clarté, cette section ne s'appliquera pas aux copies d'archives conformément à la section 2.3.3.

2.3.3 Copies d'archives. Si le Prestataire est tenu par la loi de conserver des copies d'archives des Informations Amazon à des fins fiscales ou réglementaires similaires, ces Informations Amazon archivées doivent être stockées de l'une des manières suivantes :

2.3.3.1 En tant que sauvegarde « froide » ou hors ligne (c.-à-d. non disponible pour une utilisation immédiate ou interactive) stockée dans une installation physiquement sécurisée ; ou

2.3.3.2 Chiffrée, où le système hébergeant ou stockant le ou les fichier(s) chiffrés n'a pas accès à une copie de la/des clé(s) utilisée(s) pour le chiffrement.

2.3.4 Récupération. Si le Prestataire effectue une récupération (c.-à-d., en retour à une sauvegarde) à des fins de reprise après sinistre, le Prestataire disposera et maintiendra un processus qui garantit que toutes les Informations Amazon qui doivent être supprimées conformément à l'Accord ou à la présente Politique de sécurité ou tout autre accord avec Amazon seront supprimées ou écrasées des données récupérées conformément à la présente section 2.3 dans les 24 heures suivant la récupération. Si le Prestataire effectue une récupération à quelque fin que ce soit, aucune Information Amazon ne peut être récupérée sur un système ou réseau tiers sans l'approbation écrite préalable d'Amazon. Amazon se réserve le droit d'exiger un examen de sécurité Amazon (conformément à la Section 2.5 (Examen de sécurité)) du système ou réseau tiers avant d'autoriser la récupération de toute Information Amazon sur tout système ou réseau tiers.

2.3.5 Normes de nettoyage des données. Toutes les Informations Amazon supprimées par le Prestataire seront supprimées conformément aux Recommandations de nettoyage minimum (Minimum Sanitization Recommendations) contenues dans NIST SP 800-88 Révision 1, Directives pour le nettoyage des supports (Guidelines for Media Sanitation), 18 décembre 2014 (disponibles à la page http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Annexe A, pour la purge du type de dispositif concerné. En l'absence de directives pertinentes dans la norme NIST SP 800-88, Annexe A, le dispositif contenant les Informations Amazon sera détruit de l'une des manières suivantes : (a) par démagnétisation des supports magnétiques dans un champ de flux électromagnétique de 10 000+ Gauss, (b) par déchiquetage ou désintégration mécanique qui entraîne des particules inférieures à 2x2 mm, ou (c) par le biais d'autres normes qu'Amazon peut exiger sur la base de la classification et la sensibilité des Informations Amazon.

2.4 Destruction judiciaire. Avant de disposer (de quelque manière que ce soit) de tout matériel, logiciel ou autre support contenant, ou ayant contenu à tout moment, des Informations Amazon, le Prestataire procédera à une destruction légale complète du matériel, du logiciel ou de tout autre support de sorte que la récupération des Informations Amazon, sous quelque forme que ce soit, soit impossible. Le Prestataire effectuera une destruction légale conformément aux Recommandations de nettoyage minimum (Minimum Sanitization Recommendations) contenues dans NIST SP 800-88, Annexe A, pour la destruction du type de dispositif concerné.

2.4.1 Le Prestataire s'abstiendra de vendre, revendre, donner, remettre à neuf ou autrement transférer (y compris la vente ou le transfert de tout matériel, logiciel ou autre support, toute disposition en lien avec toute liquidation de l'activité du Prestataire, ou toute autre disposition) tout matériel, logiciel ou autre support qui contient des Informations Amazon qui n'ont pas été détruites de manière légale par le Prestataire comme l'exige la présente section 2.4.

2.5 Examen de sécurité.

2.5.1 Amazon se réserve le droit de demander périodiquement au Prestataire de participer à une évaluation des risques Amazon.

2.5.2 Certification. Sur demande écrite d'Amazon, le Prestataire certifiera par écrit à Amazon que les informations fournies dans le cadre de l'évaluation des risques sont conformes à la présente Politique de sécurité convenue en dernier lieu par le Prestataire et Amazon. Dans la mesure où des modifications sont apportées à la Politique de sécurité conformément à la section 1.1, ces modifications prendront effet aux fins de la présente section seulement lors d'un accord entre le Prestataire et Amazon (un e-mail suffit).

2.5.3 Autres examens. Amazon se réserve le droit d'examiner périodiquement la sécurité des Systèmes d'information Amazon, mais pas plus d'une fois par an, sauf si (a) une déficience importante antérieure a été identifiée au cours de l'année civile ou (b) Amazon est tenu par une agence gouvernementale ou un autre organisme de réglementation d'effectuer cet examen. Le Prestataire coopérera et fournira à Amazon toutes les informations requises dans un délai raisonnable, mais pas plus de 20 jours civils à compter de la date de la demande d'Amazon.

2.5.4 Remédiation. Si un examen de sécurité identifie des déficiences, le Prestataire prendra, aux frais exclusifs du Prestataire, toutes les mesures raisonnables nécessaires pour remédier à ces déficiences dans un délai convenu.

2.6 Incidents de sécurité.

2.6.1 Le Prestataire informera Amazon dès que possible, mais au plus tard 24 heures après avoir eu connaissance d'un(e) accès, collecte, acquisition, utilisation, transmission, divulgation, corruption ou perte d'Informations Amazon ou d'une violation des Systèmes d'information Amazon (un « **Incident de sécurité** »). Le Prestataire remédiera à chaque Incident de sécurité en temps opportun et fournira à Amazon des détails écrits concernant l'enquête interne du Prestataire concernant chaque Incident de sécurité. Lorsque les lois applicables l'autorisent, le Prestataire convient de n'informer aucune autorité réglementaire ni aucun client au nom d'Amazon, à moins qu'Amazon ne le demande spécifiquement par écrit au Prestataire, et Amazon se réserve le droit d'examiner et d'approuver la forme et le contenu de toute notification avant qu'elle ne soit fournie à une partie. Le Prestataire coopérera et travaillera avec Amazon pour formuler et exécuter un plan visant à rectifier tous les Incidents de sécurité confirmés.

2.6.2 Dans la mesure permise par la loi applicable, si le Prestataire reçoit une demande ou une ordonnance d'un organisme public (tel qu'une assignation à comparaître, une ordonnance judiciaire ou un mandat de recherche) demandant des données qui incluent des Informations Amazon, le Prestataire fournira un préavis suffisant à Amazon pour lui permettre de demander une mesure conservatoire ou tout autre recours approprié.

2.7 Dispositions générales. Amazon conserve l'entière discrétion de prendre toutes les décisions applicables en vertu de la présente Politique de sécurité. Toute liste d'exemples suivant « y compris » ou « par ex. » est illustrative et non exhaustive. Toutes les références aux normes pour les exigences de sécurité en vertu de la présente Politique de sécurité font référence aux normes spécifiées et à leurs versions ultérieures respectives ou versions équivalentes, telles qu'elles peuvent être mises à jour, sauf indication contraire d'Amazon.