Exigences de sécurité informatique Nestlé

Définitions

« **Système d'IA** », un système conçu ou basé sur une machine qui peut, pour un ensemble donné d'objectifs et avec des niveaux d'autonomie variables, générer des résultats tels que des prédictions, des recommandations ou des décisions influençant des environnements réels ou virtuels.

« **Cadre Reconnu par l'Industrie** » désigne un cadre, une norme ou un système de sécurité de l'information reconnu par l'industrie, tel que la certification ISO/IEC 27001:2013 ou ISO/IEC 27001:2022 ; les rapports de contrôle d'organisation de services 2 (SOC 2) Type II, tels que SSAE 16 Type II ou ISAE 3402 Type II ; ou le cadre de cybersécurité du NIST. Le Cadre Reconnu par l'Industrie peut inclure d'autres cadres ou normes de sécurité des informations, tels que l'auto-évaluation officielle CCM de Cloud Security Alliance (CSA) ou l'auto-évaluation de la sécurité CAIQ, sur consentement écrit du Client basé sur une cote de criticité inférieure des services. Dans le cas où les Services impliquent l'utilisation de systèmes d'IA, le Cadre Reconnu par l'Industrie inclura également le cadre de gestion des risques en intelligence artificielle du NIST ou tout cadre subséquent.

« **Zone sécurisée** » désigne une zone physique contenant des données du Client auxquelles le Fournisseur, ses Affiliés ou le Sous-traitant, tels que les fournisseurs de services cloud, contrôlent, surveillent et restreignent l'accès.

1. Contrôles organisationnels

1.1. Objet, portée et évolution

1.1.1. Le Fournisseur fera en sorte que ses Affiliés et Sous-traitants mettent en œuvre et maintiennent, pendant toute la durée du présent Contrat, les mesures de sécurité énoncées dans la présente Annexe (les « Exigences de sécurité informatique ») afin de sécuriser et de protéger à tout moment la confidentialité, l'intégrité et la disponibilité des Données du Client et des Systèmes nécessaires pour fournir les Services au Client.

1.1.2. Les Exigences de sécurité informatique sont soumises aux progrès et à l'évolution techniques. À ce titre, le Fournisseur et ses Filiales et Sous-traitants peuvent mettre en œuvre des mesures alternatives adéquates, à condition toutefois que ces changements n'entraînent pas une diminution du niveau de protection.

1.1.3. Le Fournisseur fera en sorte que ses sociétés Affiliées et ses Sous-traitants :

a) documentent et informent le Client de tous les changements significatifs dans leur mise en œuvre respective des Exigences de sécurité informatique ;
b) fournissent rapidement la documentation de sécurité et les informations pertinentes supplémentaires sur demande du Client.

1.2. Programme de sécurité de l'information

Le Fournisseur fera en sorte que ses Affiliés et Sous-traitants maintiennent et appliquent un programme de sécurité de l'information comprenant des politiques, des procédures, des directives et des ressources et activités associées dans le but de protéger ses actifs d'informations (le « Programme de Sécurité de l'Information ») qui :

(i) est conçu pour se conformer à un Cadre Reconnu par l'Industrie ;

(ii) comprend des garanties organisationnelles, techniques et physiques raisonnablement conçues pour sécuriser et protéger la confidentialité, l'intégrité, la disponibilité et la sécurité des Données du Client et des Systèmes nécessaires pour fournir les Services au Client ;
(iii) est adapté au caractère sensible des informations traitées, aux risques inhérents aux Services et à la nature, à la taille et à la complexité des opérations commerciales du Fournisseur ; et
(iv) est conforme à toutes les lois applicables.

Le Fournisseur fournira au Client, à sa demande et sans frais, la documentation relative au Programme de Sécurité du Fournisseur et de ses Sous-traitants (par exemple, copie de la certification ISO 27001, la Déclaration d'applicabilité ISO).

1.3. Contrôles d'accès, identification et authentification

Le Fournisseur veillera, et obligera ses Affiliés et Sous-traitants à, maintenir et appliquer des contrôles d'accès, des procédures de gestion et des protocoles pour empêcher l'accès non autorisé aux Systèmes du Fournisseur qui traitent les Données du Client et fournissent des services au Client. En outre, le Fournisseur veillera à ce qu'une procédure de gestion de l'accès appropriée soit en place pour accorder, modifier, supprimer et examiner l'accès aux systèmes du Fournisseur.

Le Fournisseur définira les procédures et contrôles mis en place pour identifier et authentifier correctement ses employés et ceux de ses Affiliés et Sous-traitants afin de protéger et de sécuriser à tout moment la confidentialité, l'intégrité et la disponibilité des Données du Client.

Dans la mesure où les Services consistent en un Logiciel en tant que Service s'exécutant sur une Plateforme ou une Infrastructure en tant que Service (PaaS ou IaaS) et que le Fournisseur est responsable de certains ou de tous les aspects de la gestion de l'accès, le Fournisseur mettra en œuvre des contrôles de sécurité configurables pour authentifier les utilisateurs du Client conformément aux normes suivantes au minimum :

a) En cas d'accord avec le Client, le Fournisseur mettra en œuvre un Single Sign On (SSO).
b) Délai d'inactivité de la session (en minutes) compris entre 16 et 60.
c) Multi-Factor Authentication (MFA) pour tous les comptes d'administrateur ou d'accès privilégié.
d) Les informations d'identification seront stockées au repos à l'aide d'un algorithme de hachage unidirectionnel (SHA-256, sécurité équivalente ou supérieure) avec un sel.
e) Si la mise en place d'un Single Sign On (SSO) n'est pas possible, le Fournisseur mettra en œuvre les contrôles suivants ainsi que les exigences ci-dessus dans la Section 1.4.2 b), c) et d) :
    1) Durée de vie maximale du mot de passe : 90 jours.
    2) Historique des mots de passe : 8 mots de passe mémorisés.
    3) Longueur minimale du mot de passe :
        I. Comptes d'Utilisateurs Finaux : 10 caractères.
        II. Compte Privilégié : 16 caractères.
    4) Les mots de passe doivent contenir des caractères appartenant à trois des quatre catégories suivantes :
        I. Caractères en majuscules.
        II. Caractères minuscules.
        III. Base 10 chiffres.
        IV. Caractères spéciaux.

En outre, et dans la mesure où il s'agit de Services Cloud, les Services auront la possibilité d'utiliser des normes de gestion des identités et des accès telles que :

a) la SCIM et/ou l'intégration de l'API pour la création, la modification et la suppression de comptes d'utilisateurs et de permissions d'accès, et l'échange de données d'identité ; et
b) SAML, OAuth, OpenID Connect afin de prendre des décisions d'authentification et d'autorisation.

1.4. Programme de Gestion de la Continuité des Opérations

1.4.1. Le Fournisseur veillera, et obligera ses Affiliés et Sous-traitants, à maintenir un **Programme de Gestion de la Continuité des Opérations** approprié comprenant une reprise après sinistre, des stratégies de continuité des opérations, des plans, des actions ainsi qu'un plan d'urgence et des politiques et procédures connexes capables de fournir une protection ou des modes de fonctionnement alternatifs pour les activités ou les processus opérationnels, y compris, mais sans s'y limiter, la gestion des crises, la continuité des opérations et la reprise après sinistre informatique (collectivement, le « Programme GCO »).

a) **Le Plan de Gestion de Crise** comprendra des éléments tels que la gestion des événements, l'activation du plan et de l'équipe, l'événement et la documentation du processus de communication dans le but d'atténuer la crise et d'en réduire l'impact.
b) **Le Plan de Continuité d'Activité** comprendra des informations documentées qui aideront le Fournisseur à répondre à une interruption et à reprendre, récupérer et restaurer la prestation de services conformément à ses objectifs de continuité d'activité.
c) **Le Plan de Reprise d'Activité Après Sinistre Informatique** inclut la stratégie conçue pour la reprise après un sinistre, une interruption d'activité ou une crise affectant l'infrastructure, la technologie, les systèmes et les activités de reprise, et identifie les personnes et les équipes requises pour une telle reprise.

Le Fournisseur révisera le Programme de Gestion de la Continuité des Opérations au moins une fois par an ou lorsque des changements importants sont apportés aux processus opérationnels et assurera la continuité des opérations en cas de catastrophe affectant les opérations opérationnelles du Fournisseur sans réduction ou dégradation substantielle des fonctionnalités ou de la disponibilité.

1.4.2. Le Fournisseur testera au moins une fois par an toutes les fonctionnalités de Programme de Gestion de la Continuité des Opérations et fournira les résultats de ces tests au Client sur demande écrite. Le Fournisseur traitera et corrigera rapidement et sans retard injustifié les erreurs ou les problèmes importants identifiés lors des tests annuels de son programme GCO.

1.4.3. En cas d'erreurs de traitement des données ou de perte de données causées par un acte ou une omission du Fournisseur ou de ses Sous-traitants, le Fournisseur informera rapidement le Client de ces cas, les corrigera à ses frais et suivra les stratégies de gestion de la continuité des opérations appropriées. En cas d'erreurs de traitement causées par le Client ou un tiers, le Fournisseur les corrigera sur notification écrite au Client.

1.5. Réponse aux Incidents de Sécurité des Informations

1.5.1. Le Fournisseur doit mettre à jour et réviser au moins une fois par an ou lorsqu'un changement important se produit les politiques et procédures de gestion des incidents de sécurité capables d'identifier et d'atténuer les effets des Incidents de Sécurité de l'Information, y compris les procédures détaillées de remontée des incidents de sécurité. En cas d'Incident de Sécurité des Informations, le Fournisseur devra, à ses frais :

a) signaler rapidement (mais en aucun cas plus de vingt-quatre (24) heures après que le Fournisseur ou son Affilié ou Sous-traitant (ou les membres de leur personnel respectif) a pris connaissance d'un Incident de Sécurité des Informations) cet Incident de Sécurité des Informations au Centre de Sécurité des Clients, qui fonctionne 24x7 et peut être contacté au +41 21 924 91 91 ou à l'adresse gsoc@nestle.com, en résumant de manière raisonnablement détaillée l'effet sur le Client et ses Affiliés (si connu), et en fournissant au Client des canaux de communication ininterrompus avec l'équipe de sécurité des informations du Fournisseur indépendamment de toute communication parallèle entre les Parties ;
b) enquêter (avec la participation du Client et/ou d'un enquêteur judiciaire tiers indépendant) sur un tel Incident de Sécurité des Informations, effectuer une évaluation des risques et développer un plan de mesures correctives ;

c) fournir au Client un rapport écrit de l'évaluation des risques et du plan d'action entrepris ou à entreprendre par le Fournisseur. En cas d'atteinte aux lois ou règlements applicables, une analyse juridique devrait être incluse ;
d) préparer et mettre en œuvre un plan de mesures correctives pour prendre toutes les mesures correctives nécessaires et recommandées et coopérer pleinement avec le Client et toutes les sociétés affiliées du Client dans tous les efforts raisonnables et légaux visant à prévenir, atténuer, rectifier et remédier aux effets de l'incident de sécurité des informations ;
e) au terme des actions d'enquête, de correction et de remédiation relatives à l'incident de sécurité de l'information, un rapport écrit final comprenant des détails raisonnables sur : (i) la nature et la gravité de l'Incident de Sécurité de l'Information ; (ii) les Données Clients divulguées, détruites, compromises ou altérées ; (iii) toutes les actions correctives effectuées ; et (iv) tous les efforts déployés pour atténuer les risques d'Incidents de Sécurité de l'Information à l'avenir.

1.5.2. Le Fournisseur testera toutes les caractéristiques de ses procédures du Programme de Réponse aux Incidents de Sécurité des informations au moins une fois par année civile. En cas d'accord écrit avec le Client, le Fournisseur fournira les résultats de ces tests au Client sur demande.

2. Contrôles technologiques

2.1. Contrôles cryptographiques

Le Fournisseur obligera ses Affiliés et Sous-traitants à mettre en œuvre et à utiliser des protocoles, algorithmes et techniques de cryptage standard pour protéger la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation des Données du Client comme suit :

a) En mouvement, y compris au sein de réseaux publics et privés, en utilisant une puissance de schéma de chiffrement d'au moins 256 bits pour le chiffrement symétrique ou d'au moins 2048 bits pour le chiffrement asymétrique.
b) Au repos, y compris les sauvegardes éventuelles, en utilisant une puissance de schéma de chiffrement d'au moins 256 bits pour le chiffrement symétrique ou d'au moins 2 048 bits pour le chiffrement asymétrique.

2.2. Activités de monitoring

Le Fournisseur fera en sorte que ses Affiliés et Sous-traitants surveillent activement les Services et les Systèmes pour tout accès non autorisé, interception ou interruption à l'aide d'outils ou de mécanismes de sécurité standard acceptés de l'industrie pour générer, surveiller et répondre aux alertes qui pourraient indiquer une compromission potentielle du réseau et/ou de l'hôte, et d'autres contrôles de sécurité qui fournissent une surveillance continue, ont la capacité de restreindre le trafic réseau non autorisé, de détecter et de limiter l'impact des attaques.

Le Fournisseur utilisera, et fera en sorte que ses Affiliés et Sous-traitants utilisent, des contrôles de prévention des fuites de données conçus pour surveiller et/ou empêcher la compromission involontaire ou intentionnelle des Données du Client. Les contrôles permettent de suivre l'activité, de surveiller le trafic réseau et les e-mails d'entreprise, et de filtrer/bloquer les actions des utilisateurs pour garantir la sécurité des Données Client.

2.3. Segmentation du réseau

Les Données du Client sont et resteront la propriété exclusive du Client. Le Fournisseur maintiendra des mesures de segmentation du réseau basées sur des normes acceptées par l'industrie pour restreindre l'accès au réseau aux systèmes stockant les Données du Client et s'assurera que toutes les données mises à disposition par le Client au Fournisseur ou à l'une de ses Filiales ou Sous-traitants seront, par des moyens

techniques appropriés, tenues logiquement séparées des données du Fournisseur et des données de tout autre Client du Fournisseur ou de ses Filiales ou Sous-traitants.

2.4. Accès et connexion à distance

Le Fournisseur mettra en œuvre des contrôles d'accès à distance pour ses systèmes publics ou privés afin de restreindre l'accès des personnes non autorisées et de protéger les Données du Client. Le Fournisseur n'autorisera pas les connexions directes non sécurisées des réseaux publics vers un segment de réseau interne. Ces contrôles et ces mesures de protection visent notamment à assurer :

(i) L'Authentification multifacteur ;
(ii) Le tunneling fractionné n'est autorisé à aucun moment lors de la connexion à distance aux réseaux du Fournisseur ; et
(iii) Les utilisateurs distants sont réexaminés au moins une fois par an en vue d'une nouvelle certification.

Lorsque le Fournisseur se connecte à distance au réseau du Client et/ou accède à distance aux systèmes publics ou privés du Client, directement à partir d'Internet ou en utilisant des technologies VPN ou toute autre méthode de connexion, le Fournisseur reconnaît et accepte que :

a) Tout le trafic réseau et tous les accès aux données et systèmes du Client sont consignés et peuvent être surveillés ;
b) L'Authentification multifacteur est requise pour l'accès à distance aux Systèmes publics ou privés du Client ;
c) La connexion au réseau est uniquement un moyen de partager certaines données entre le Fournisseur et le Client et de faciliter la fourniture de Services au Client ;
d) Le Fournisseur est responsable de toutes les données et/ou modifications publiées par ou pour le compte du Fournisseur, et le Client ne sera pas tenu responsable, ou n'aura aucune obligation de surveiller ou de maintenir une supervision concernant ces modifications ou ces données ;
e) Le Client fera tous les efforts commercialement raisonnables pour sécuriser ses systèmes et réseaux en appliquant les meilleures pratiques et normes du secteur ;
f) Le Fournisseur sera responsable de la sécurité de son utilisation de la connexion (et de l'utilisation de la connexion par le personnel du Fournisseur et les sous-traitants), de l'utilisation de l'environnement informatique du Client et/ou de l'utilisation des données du Client ; et
g) Lorsque des informations d'identification sont attribuées par le Client aux utilisateurs autorisés du Fournisseur, ces informations sont confidentielles et personnelles pour chaque utilisateur individuel et ne peuvent être divulguées pour quelque raison que ce soit.

Le Fournisseur ne créera pas de portes dérobées ou de programmes similaires qui pourraient être utilisés pour accéder aux systèmes et/ou aux données Client, y compris, mais sans s'y limiter, les systèmes qui traitent les Données du Client.

Avant de recevoir les Données du Client, le Fournisseur s'assurera que les Lois applicables n'exigent pas du Fournisseur qu'il crée ou entretienne des portes dérobées ou qu'il facilite l'accès aux Données ou aux Systèmes du Client ou que le Fournisseur soit en possession de la clé de chiffrement ou qu'il la divulgue. Dans le cas où le Fournisseur ne serait plus en mesure de satisfaire à ces exigences, il informera rapidement le Client, dans toute la mesure permise par les Lois applicables, et respectera les instructions du Client en ce qui concerne la sécurité, la suppression, le retour, le chiffrement ou tout autre traitement des Données du Client.

2.5. Journalisation

Le Fournisseur aura mis en place un programme complet de gestion des journaux définissant la portée, la génération, la transmission, le stockage, l'analyse et l'élimination des journaux relatifs aux services basés

sur un Cadre Reconnu par l'Industrie. Les Systèmes et les Services fourniront des capacités de journalisation conformément aux principes suivants :

a) des journaux d'audit seront conservés indiquant à chaque fois quand les données du Client ont été consultées et par qui ;
b) le champ d'application de l'enregistrement et la politique de rétention seront fondés sur une approche basée sur les risques ;
c) les journaux seront suffisants pour permettre des investigations numériques des incidents de sécurité de l'information, y compris les activités, les exceptions, les pannes et autres événements pertinents qui devraient être produits, stockés et protégés, afin de soutenir les enquêtes et aider à identifier les activités inhabituelles ou les comportements anormaux qui peuvent représenter des indicateurs de compromission ;
d) les journaux enregistreront les modifications administratives apportées aux Services ;
e) les registres seront tenus physiquement et virtuellement en lieu sûr pour empêcher toute manipulation;
f) les mots de passe ne seront enregistrés en aucun cas ; et
g) en cas accord avec le Client, l'intégration de l'API sera disponible pour transférer les données vers la plate-forme SIEM du Client si nécessaire.

Le Fournisseur s'engage à ce que ses Affiliés et Sous-traitants fournissent au Client des copies de tous les fichiers journaux raisonnablement demandés pour l'aider dans l'analyse ou l'investigation des Incidents de Sécurité des Informations.

2.6. Protection contre les logiciels malveillants

Le Fournisseur fera en sorte que ses Affiliés et Sous-traitants utilisent des mesures standard de l'industrie pour empêcher les Services d'introduire, de permettre ou de faciliter l'introduction de Code Malveillant dans les Systèmes. À cette fin, le Fournisseur :

a) installera et mettra à jour régulièrement un logiciel de détection et de réparation de logiciels malveillants standard et, dans la mesure du possible, utiliser des fonctions de protection en temps réel ;
b) maintenir le logiciel de détection et de réparation de logiciels malveillants conformément aux pratiques recommandées par le Fournisseur du logiciel de détection et de réparation de logiciels malveillants pour empêcher les systèmes et/ou les services d'être infectés ou affectés par la présence de Code Malveillant ;
c) corriger immédiatement tout Code Malveillant découvert ou susceptible d'être présent dans les Systèmes ou les Services ;
d) et effectuer une analyse en temps réel des fichiers et autres données téléchargés dans les Services pour identifier et corriger tout fichier ou autre donnée contenant du Code Malveillant.

2.7. Gestion des risques liés aux systèmes d'IA

Dans la mesure où les Services fournis par le Fournisseur dans le cadre du présent Contrat impliquent des Systèmes d'IA pour le traitement des Données du Client, le Fournisseur obligera ses Affiliés et Sous-traitants à mettre en œuvre, maintenir et appliquer un cadre de sécurité complet adhérant au minimum à un Cadre Reconnu par l'Industrie pour assurer la confidentialité, l'intégrité et la disponibilité des Données du Client et la conformité à toutes les Lois applicables (le Cadre de Sécurité d'IA).

À la demande du Client, le Fournisseur fournira au Client des rapports réguliers sur la mise en œuvre et l'efficacité du Cadre de sécurité de l'IA, y compris des preuves de conformité au Cadre Reconnu par l'Industrie.

2.8. Procédures de backup

Le Fournisseur devra :

a) s'assurer que les Données du Client sont sauvegardées et stockées dans un emplacement et un format disponible pour la récupération en cas de besoin ;
b) sauvegarder des copies des Données du Client et des procédures de récupération des données dans un endroit différent de celui où se trouve l'équipement informatique principal traitant les Données du Client ;
c) avoir mis en place des procédures spécifiques régissant l'accès aux copies des Données du Client ;
d) examiner et mettre à l'essai les procédures de récupération des données au moins tous les six (6) mois ou lorsqu'un changement important se produit ; et
e) consigner les efforts de restauration des données, y compris la personne responsable, la description des données restaurées et les données (le cas échéant) qui ont dû être saisies manuellement dans le processus de restauration des données.

2.9. Évaluations et audits de sécurité

2.9.1. Programme de gestion des vulnérabilités

Le Fournisseur disposera d'un programme complet de gestion des vulnérabilités, qu'il examinera chaque année ou lorsqu'un changement important se produira, et qui garantira l'identification, la catégorisation et la correction en temps opportun des vulnérabilités techniques et des processus au niveau de l'infrastructure et des applications du ou des systèmes. Le programme de gestion des vulnérabilités sera basé sur un Cadre Reconnu par l'Industrie et comprendra une surveillance proactive des menaces de sécurité informatique externes et/ou internes qui peuvent potentiellement causer un Incident de Sécurité de l'Information ou nuire aux Systèmes et/ou Services.

Le Fournisseur s'assurera que les correctifs logiciels pour corriger les vulnérabilités sont installés et activés dans les délais suivants et selon la classification de gravité des vulnérabilités :

a) Critique : immédiatement au plus tard 7 jours civils.
b) Élevé : dès que possible, au plus tard dans les 30 jours civils.
c) Moyenne : prochaine mise à jour de sécurité, au plus tard 90 jours civils.

Le Fournisseur identifiera et communiquera au Client toute contrainte ayant un impact sur la capacité à remédier à la vulnérabilité dans le délai convenu.

Aux fins de la présente Section, la définition de la gravité des vulnérabilités relevées (c.-à-d. critiques, élevées, moyennes ou faibles) sera fondée sur les normes de l'industrie, comme le « Common Vulnerability Scoring System » (CVSS) fourni par le « Forum of Incident Response and Security Teams » (FIRST).

2.9.2. Test d'intrusion

Le Fournisseur engagera, à ses propres frais, un tiers indépendant sur une base annuelle pour mener et rapporter les résultats des tests d'intrusion, y compris des tests manuels humains, pour évaluer les contrôles de sécurité de l'application (y compris, mais sans s'y limiter, les services Web et les applications mobiles), les couches hôte et réseau utilisées pour fournir les Services selon les méthodologies standard de l'industrie (par exemple, OWASP et OSSTMM).

Le Fournisseur fournira gratuitement au Client, à sa demande, des copies du rapport. Le Fournisseur informera rapidement le Client de tout défaut identifié ainsi que des mesures correctives nécessaires pour corriger toutes les vulnérabilités. Si une vulnérabilité critique est identifiée, le Fournisseur entreprendra des actions correctives dans les sept (7) jours civils suivant la réception du rapport, et incitera ses Affiliés et Sous-traitants à le faire. Si une vulnérabilité élevée est décelée, des mesures correctives seront prises par

le Fournisseur et ses Affiliés et Sous-traitants (le cas échéant) dans les trente (30) jours civils suivant la réception du rapport.

Aux fins de la présente Section, les définitions de la gravité des vulnérabilités relevées (c.-à-d. critiques, élevées, moyennes ou faibles) seront fondées sur des normes de l'industrie comme la « Risk Rating Methodolog » de l'OWASP ou le « Common Vulnerability Scoring System » (CVSS).

2.9.3. Conformité PCI

Si le Fournisseur gère les processus liés à PCI.

Le Fournisseur se conformera à ses propres frais à la dernière version de la norme de sécurité des données de l'industrie des cartes de paiement (« PCI DSS »). En cas de conflit entre le PCI DSS et les termes du présent accord, le PCI DSS prévaudra dans la mesure nécessaire pour se conformer à ces exigences.

Si le Fournisseur est inscrit en tant que prestataire de services marchand sur la liste des prestataires de services Visa ou sur la liste des prestataires de services enregistrés conformes à la Protection des Données des Sites Mastercard (PDS), le Fournisseur doit fournir une Attestation de Conformité PCI (AC) telle que définie par le Conseil de Sécurité PCI (dernière version disponible sur https://www.pcisecuritystandards.org) avant de traiter les paiements par carte. Par la suite, à condition qu'un enregistrement Visa ou Mastercard approprié soit maintenu, le Fournisseur ne fournira une AC qu'en cas de modification importante de l'étendue des services du Fournisseur ou des conditions de l'AC.

Le Fournisseur comptabilisera le nombre de transactions par carte traitées pour le compte de tous les Clients dans le monde et fournira au Client, sur demande, des informations permettant de contrôler la conformité.

Si le Fournisseur stocke, traite et/ou transmet plus de 300 000 transactions de compte par an (Fournisseur de services de niveau 1), il fournira, sur une base annuelle et par la suite, une AC tel que définie par le Conseil des Normes de Sécurité PCI (la dernière version disponible sur https://www.pcisecuritystandards.org), comme requis par les règles de validation VISA™ et MasterCard™. En outre, le CEA doit également être contresigné par un Evaluateur de Sécurité Qualifié (ESQ) actif et autorisé si une auto-évaluation (SAQ D) est utilisée au lieu d'une évaluation sur place (ROC).

Si le Fournisseur stocke, traite et/ou transmet moins de 300 000 transactions de compte par an (Fournisseur de services de niveau 2), il fournira, sur une base annuelle et par la suite, une AC tel que défini par le Conseil des Normes de Sécurité PCI (la dernière version disponible sur https://www.pcisecuritystandards.org), comme requis par les règles de validation VISA™ et MasterCard™. Lorsque le Fournisseur utilise une SAQ D sans recourir aux services d'un ESQ autorisé, il incombe au Fournisseur de s'assurer que la personne qui effectue l'évaluation est compétente pour le faire. Si l'AC ou la SAQ-D sont jugés non conformes à la norme PCI en ce qui concerne les services fournis, le Fournisseur disposera de 90 jours pour y remédier. Dans le cas où le Fournisseur ne peut pas corriger l'AC ou la SAQ-D à un niveau de conformité, le Fournisseur sera invité à engager un Évaluateur de Sécurité Qualifié (ESQ) autorisé à ses propres frais et à effectuer les activités correctives nécessaires pour atteindre une AC signée par un ESQ.

Le Fournisseur informera le Client dans les 24 heures de tout changement dans son état de conformité PCI DSS ou de la découverte de toute violation de données suspectée impliquant des données, y compris des données de titulaire de carte, qui lui sont fournies en vertu du présent Contrat.

Pour éviter toute ambiguïté, le Fournisseur reconnaît qu'il est responsable de la sécurité de toutes les données du titulaire de la carte qui lui sont fournies en vertu du présent Contrat.

3. Contrôles physiques

3.1. Sécurité physique

Les mesures de sécurité physique s'appliquent à toutes les installations où les Données du Client sont traitées pour fournir le Service. Le Fournisseur et ses Fournisseurs de services cloud protégeront leurs propriétés et leurs actifs contre les accès qui présentent un risque potentiel pour les données du Client, sécuriseront et surveilleront l'accès à toute Zone Sécurisée et maintiendront des contrôles de sécurité physiques au niveau de la Zone Sécurisée.

3.1.1. Zone sécurisée gérée par le Fournisseur

Toutes les installations contenant les Systèmes doivent au moins :

a) être structurellement conçus pour résister à des conditions météorologiques défavorables et à d'autres conditions naturelles raisonnablement prévisibles ;
b) avoir des mesures de protection physique appropriées de l'environnement pour protéger les systèmes contre les dommages liés à la fumée, à la chaleur, à l'eau, au feu, à l'humidité ou aux fluctuations de l'alimentation électrique ;
c) être pris en charge par des Systèmes de production d'énergie de secours sur place ;
d) disposer de contrôles appropriés pour garantir que seul le Personnel autorisé du Fournisseur est autorisé à accéder physiquement à l'installation.

3.1.2. Zone sécurisée gérée par le Fournisseur de services cloud

Le Fournisseur garantit et déclare que le Fournisseur de services cloud maintiendra des contrôles de sécurité physiques conçus pour se conformer à un Cadre Reconnu par l’Industrie et pour répondre aux exigences réglementaires applicables.

3.2. Elimination des supports

Le Fournisseur utilisera des processus conformes aux normes de l'industrie, tels que décrits dans les Cadres Reconnus de l'Industrie, pour éliminer les supports contenant les données du Client (p. ex., Fournisseur de services certifiés d'élimination des supports).

4. Contrôles des personnes

4.1. Sensibilisation

Le Fournisseur doit s'assurer que ses employés, ainsi que ceux de ses Affiliés et/ou Sous-traitants, engagés dans la fourniture de Services, connaissent toutes les politiques, procédures et exigences réglementaires pertinentes liées aux Services et ont reçu une formation appropriée sur les obligations pertinentes en vertu du présent Contrat.

4.2. Formation

Le Fournisseur garantit que son personnel recevra des informations concernant les procédures et les contrôles raisonnablement nécessaires pour se conformer au présent Contrat. Le Fournisseur doit fournir à son personnel une formation périodique de sensibilisation à la sécurité qui couvre, au minimum : (i) la sécurité de l'information ; (ii) la protection de la vie privée ; et (iii) la continuité des activités.