Exigences de sécurité Nestlé

1. Applicabilité et évolution

1.1. Le Fournisseur s'engage et fera en sorte que ses Affiliés et ses Sous-traitants s'engagent à mettre en oeuvre et maintenir pendant toute la durée du présent Contrat les mesures de sécurité énoncées dans la présente Annexe (les "Exigences de sécurité") afin de garantir à tout moment la confidentialité, l'intégrité et la disponibilité des Données du Client.

1.2. Les Exigences de sécurité sont sujettes au progrès technique et à l'évolution. À ce titre, le Fournisseur, ses Affiliés et ses Sous-traitants peuvent mettre en oeuvre des mesures de remplacement adéquates ; à condition toutefois que le niveau de sécurité ne soit jamais réduit.

1.3. Le Fournisseur s'engage et fera en sorte que ses Affiliés et ses Sous-traitants s'engagent (a) à consigner et informer le Client de tous les changements importants dans leur mise en oeuvre respective des Exigences de sécurité et (b) fournir rapidement toute information supplémentaire pertinente, sur demande du Client.

2. Normes de sécurité

2.1. Le Fournisseur s'engage et fera en sorte que ses Affiliés et ses Sous-traitants s'engagent à maintenir : (a) une certification ISO/IEC 27001 (ou un rapport équivalent conforme aux normes de l'industrie accepté par le Client) (la "certification ISO 27001") ou (b) un rapport de contrôle de type « Service Organisation Control 2 », « Type II report », tel que SSAE 16 Type II ou ISAE 3402 Type II (ou tout rapport équivalent accepté par le Client) (le "Rapport SOC 2"), et ce dans chaque cas pour la sécurité, la disponibilité, l'intégrité, la confidentialité et les contrôles liés à la protection des données personnelles au sein des systèmes d'information (y compris les procédures, les personnes, les logiciels, les données, les données, les logiciels) qui sont utilisés par le Fournisseur et par ses Filiales et Sous-traitants dans le traitement des données du Clients.

2.2. Le Fournisseur fournira au Client rapidement, sur demande, une copie de la certification ISO 27001, ainsi que la déclaration d'applicabilité ISO « Statement of Applicability » (SoA) ou le Rapport SOC 2. Dans la mesure où les services Cloud sont constitués d'une solution SaaS (Software-as-a-Service) s'exécutant sur la plate-forme ou l'infrastructure en tant que service (PaaS ou IaaS), le Fournisseur fournira la certification ISO27001 de l'environnement d'hébergement, ainsi que le rapport SoA ou SOC 2 au Client, rapidement et suite à sa demande.

2.3. Le Fournisseur informera rapidement le Client de tout manquement relevé dans ces certifications ou rapports. Le Fournisseur remédiera à ces manquements et les corrigera dans la mesure du nécessaire et dans le but de se conformer aux obligations du Fournisseur en vertu du présent Contrat et avisera le Client lorsque de tels manquements seront résolus. Si un manquement n'est pas résolu rapidement, il sera considéré par le Client comme une violation importante du présent Contrat de la part du Fournisseur.

3. Détection et prévention des intrusions

Le Fournisseur, ou un tiers autorisé par le Fournisseur, surveillera activement les Services et les Systèmes pour tout accès, interception ou interruption non autorisés, en utilisant des mécanismes de détection ou de prévention des intrusions en réseau reconnus, y compris les pare-feu d'application Web (WAF).

4. Test de pénétration

4.1. Le Fournisseur engagera, à ses propres frais, un tiers indépendant sur une base annuelle pour effectuer des tests de pénétration et obtenir un rapport des résultats de ces tests, y compris des tests réalisés manuellement, afin d'évaluer les contrôles de sécurité de l'application (y compris, mais sans s'y limiter, les services Web et les applications mobiles), des serveurs et des réseaux utilisés pour fournir les services selon les méthodologies standard de l'industrie (par exemple, OWASP et OSSTMM).

4.2. Le Fournisseur fournira au Client des copies dudit rapport rapidement et sur sa demande. Le Fournisseur informera rapidement le Client de toute défaillance décelée ainsi que des mesures

correctives nécessaires pour corriger toutes les vulnérabilités. Si un manquement critique est décelé, le Fournisseur prendra des mesures correctives dans les sept (7) jours civils suivant la réception du rapport et fera en sorte que ses Affiliés et ses Sous-traitants prennent les mesures correctives qui s'imposent. Si un manquement important est décelé, des mesures correctives seront prises par le Fournisseur et ses Sociétés Affiliées et Sous-traitants (le cas échéant) dans les trente (30) jours civils suivant la réception du rapport.

4.3. 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 méthodologie d'évaluation des risques du PSAMP.

5. Gestion des identités

5.1. Le Fournisseur autorisera les utilisateurs autorisés à accéder aux services uniquement après l'authentification avec des informations d'identification valides.

5.2. 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.

5.3. Les Services prestés par le Fournisseur devront contenir, le cas échéant, des contrôles de sécurité configurables conformes à la norme suivante du Client, au minimum, comme décrit ci-dessous :

1. Gouvernance de l'identité et de l'accès	Un processus de GAI officiel et documenté doit être en place pour répondre aux exigences ci-dessous.
2. Enregistrement et désenregistrement des utilisateurs	Un processus officiel d'enregistrement et de désenregistrement des utilisateurs doit être mis en oeuvre pour gérer la création de comptes et l'attribution de droits d'accès sur les systèmes. Les exigences suivantes s'appliquent : a) Chaque utilisateur doit avoir une identité numérique unique mappée à son(s) compte(s) d'utilisateur nommé(s). b) Les identités numériques doivent être recertifiées tous les six mois. c) Un interlocuteur unique interne chez Nestlé (SPOC) doit être responsable de la gestion des demandes de création, de mise à jour et de suppression de comptes pour les sociétés affiliées, les utilisateurs B2B et les utilisateurs tiers. d) Les comptes non utilisés pendant 90 jours doivent être désactivés et/ou supprimés. e) Les rapports doivent être facilement accessibles pour permettre l'examen des comptes et des autorisations d'accès (p. ex., pour s'assurer que les droits d'accès sont appropriés, pour identifier les comptes qui ne sont plus requis, etc.). f) Le cas échéant, les comptes privilégiés doivent avoir une identité numérique associée et un compte d'utilisateur nommé afin d'accéder aux environnements Nestlé. g) L'administration partagée privilégiée ou les comptes racines ne sont autorisés que s'ils sont stockés en toute sécurité dans une solution de coffre-fort. h) Lors du processus de création du compte, les mots de passe ne doivent pas être communiqués avec les noms d'utilisateurs ; des communications séparées doivent être envoyées. i) Les mots de passe fournis pour l'accès initial au compte ou pour faciliter la réinitialisation du mot de passe doivent être uniques et définis pour expirer lors de l'utilisation initiale.

3. Gestion des accès utilisateur	Un processus formel d'attribution d'accès utilisateur doit être mis en oeuvre pour attribuer ou révoquer les droits d'accès de tous les types d'utilisateurs à tous les systèmes et services. Les exigences suivantes s'appliquent : a) Les droits d'accès doivent être approuvés avant d'être accordés. b) La séparation des tâches (Segregation of Duties / SOD) doit être appliquée aux approbations. La personne qui demande ou reçoit l'accès ne doit pas donner d'approbation. c) Les enregistrements de l'attribution des droits d'accès et de l'historique des approbations doivent être conservés. d) Les droits d'accès des utilisateurs qui ont changé de rôle ou d'emploi doivent être adaptés dans les 15 jours pour refléter les responsabilités de la nouvelle fonction, à moins que des approbations ne soient données pour maintenir l'accès pour une période de temps prédéterminée. e) Les droits d'accès doivent être immédiatement supprimés ou désactivés pour les utilisateurs qui ne sont plus employés ou engagés par Nestlé. f) Les droits d'accès critiques/sensibles doivent être re-certifiés au moins une fois par an.
4. Gestion des accès privilégiés	L'attribution et l'utilisation des droits d'accès privilégiés doivent être surveillées et contrôlées au moyen d'un processus d'autorisation officiel (processus de gestion des accès privilégiés). Les exigences suivantes s'appliquent : a) Les droits d'accès privilégiés associés à chaque système ou processus (p. ex. système d'exploitation, système de gestion de base de données) doivent être clairement identifiés. b) Toutes les demandes d'accès privilégié doivent spécifier l'objet de la demande. c) Les droits d'accès privilégiés doivent être attribués, dans la mesure du possible, à un compte d'utilisateur différent de ceux utilisés pour les activités commerciales courantes, authentifiés par authentification multifacteur et inversement (par exemple, les activités commerciales régulières ne doivent pas être exécutées à partir de comptes privilégiés). d) La gestion de l'accès privilégié à des données, ordinateurs ou réseaux restreints doit permettre d'identifier la personne qui effectue l'activité à tout moment, par exemple via un compte d'utilisateur/mot de passe unique. e) Les droits d'accès privilégiés doivent être attribués aux utilisateurs selon le besoin d'utilisation. f) Les droits d'accès privilégiés doivent être revérifiés tous les six mois.
5. Gestion générique des comptes	L'attribution et l'utilisation de comptes génériques doivent être surveillées et contrôlées. Les exigences suivantes s'appliquent : a) Les comptes génériques doivent avoir un employé Nestlé identifié comme propriétaire. b) Les comptes génériques doivent contenir une description claire de leur objet et de leur fonction, c'est-à-dire des activités entreprises par le compte. c) Les comptes génériques ne doivent pas être utilisés comme compte d'utilisateur final principal d'une personne. d) La confidentialité des mots de passe doit être préservée lorsqu'ils sont partagés (par exemple, changer les mots de passe dès que possible lorsqu'un utilisateur privilégié quitte ou change de travail, communiquer le mot de passe aux utilisateurs privilégiés par des mécanismes sécurisés, etc.).

e) Lorsque vous demandez la création, la modification ou la suppression d'un compte d'utilisateur générique, les processus d'approbation appropriés doivent être suivis en fonction du type et de l'utilisation du compte.

f) Les comptes génériques doivent être re-certifiés au moins une fois par an et supprimés lorsqu'ils ne sont plus requis.

g) Toutes les demandes de privilèges d'accès au compte générique doivent spécifier l'objectif de ces privilèges d'accès. L'accès appliqué à tout compte doit suivre la notion de "privilège minimum" et doit être conforme aux activités entreprises par le compte.

h) Les comptes génériques peuvent avoir leur mot de passe défini sur "N'expire jamais".

i) Les comptes/mots de passe de solution par défaut fournis par le fournisseur doivent être modifiés, supprimés ou désactivés.

6. Système de gestion des mots de passe

Les systèmes doivent être configurés de manière à assurer la transmission et le stockage sécurisés des mots de passe par :

a) Ne pas afficher à l'écran un mot de passe saisi ;

b) Ne pas transmettre de mots de passe en texte clair sur un réseau ;

c) Application de la force du mot de passe, de la fréquence des changements, etc., exigences selon le tableau ci-dessous :

Mot de passe requis	Employés Entrepreneurs	Sociétés affiliées	Business-to-Business	Fournisseur tiers	
Longueur minimale	10				
Majuscule Caractères (A-Z)	Oui				Le mot de passe doit répondre à au moins trois de ces critères
MINUSCULE Caractères (a-z)	Oui				
Chiffres (0-9)	Oui				
Caractères spéciaux ~ ! @ # $ % ^ & * _ - + = | \ ( ) { } [ ] : ; " ' < > , ? / et tous les autres caractères Unicode autorisés par votre clavier	Oui				
Histoire	8				
Nombre de tentatives autorisées avant le verrouillage	5				
Expiration de la session inactive	15 min				
Modifier la fréquence	90 jours				
Les mots de passe pour les systèmes ou applications ne pouvant pas répondre à l'exigence de mot de passe doivent augmenter la longueur du mot de passe. -> *Longueur des caractères, si possible — et intégration de la complexité maximale que le système ou l'application peut prendre en charge*	16				

Mot de passe requis	Comptes privilégiés	Comptes Génériques	
Longueur minimale	16	16	
Majuscule Caractères (A-Z)	Oui	Oui	Le mot de passe doit répondre à trois de
MINUSCULE Caractères (a-z)	Oui	Oui	

	Chiffres (0-9)	Oui	Oui	ces critères
	Caractères spéciaux ~ ! @ # $ % ^ & * _ - + = | \ ( ) { } [ ] : ; " ' < > , ? / et tous les autres caractères Unicode autorisés par votre clavier	Oui	Oui	
	Histoire	8	8	
	Nombre de tentatives autorisées avant le verrouillage / effacement	5	5	
	Expiration de la session inactive			
	Modifier la fréquence	90 jours	Au moins une fois par an	
	Les mots de passe pour les systèmes ou applications ne pouvant pas répondre à l'exigence de mot de passe doivent augmenter la longueur du mot de passe. -> *Longueur des caractères, si possible — et intégration de la complexité maximale que le système ou l'application peut prendre en charge*	24	24	

7. Mots de passe dans le code source et les scripts

Dans le code source, les exigences suivantes s'appliquent :

a) Les mots de passe ne doivent jamais être codés en dur dans les logiciels, applications, systèmes ou services développés ou modifiés (y compris les scripts, les fichiers de commandes, etc.).

b) Les scripts de connexion, y compris les paramètres de profil, la documentation et les fichiers de commandes ne doivent pas contenir de mots de passe.

8. Utilisation du mot de passe

Les utilisateurs doivent respecter les principes suivants :

a) Les informations d'identification de l'utilisateur (compte nommé) ne doivent jamais être partagées avec quiconque.

b) Tous les mots de passe doivent être uniques quel que soit le système d'un domaine logique (par exemple, le mot de passe du même compte utilisé en production et en préproduction doit être différent).

c) Ils doivent signaler à leur organisation locale GLOBE Nestlé (LGO) tout soupçon de compromission de leur compte et prendre des mesures pour changer le mot de passe immédiatement.

d) Si nécessaire, les mots de passe doivent être stockés en toute sécurité à l'aide d'un coffre-fort avec des outils de chiffrement approuvés.

e) Les mots de passe ne doivent pas :

   a. Contiennent des renseignements personnels identifiables, comme le nom des enfants, les passe-temps, les équipes sportives préférées, le numéro de permis, la date de naissance de l'utilisateur, le nom de l'animal de compagnie, etc.
   b. Contient les noms des marques Nestlé ou des mots clés Nestlé connus, tels que Nestlé, Nespresso, etc.
   c. Avoir plus de deux caractères ou mots identiques dans une rangée, p. ex. abb1122.
   d. Inclure le nom d'utilisateur ou de connexion.
   e. Être une séquence de clavier courante, telle que "qwerty89" ou "abc123".
   f. Être un seul mot trouvé dans le dictionnaire (dans n'importe quelle langue), qu'il soit orthographié vers l'avant ou vers l'arrière, ou un seul mot précédé ou suivi d'un chiffre (p. ex. secret1, 1secret).

5.4. Dans la mesure où il s'agit de services Cloud, les services pourront utiliser les normes de gestion de l'identité et de l'accès telles que :

a) SCIM et/ou rendre l'intégration API disponible pour la création, la modification et la suppression de comptes d'utilisateurs et d'autorisations 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.

6. Réponse aux incidents de sécurité des informations

6.1. Le Fournisseur doit tenir à jour et examiner au moins une fois par an ou lorsqu'un changement important se produit les politiques et procédures de gestion des incidents de sécurité, y compris les procédures détaillées de remontée des incidents de sécurité. En cas d'incident lié à la sécurité des informations, le Fournisseur, à ses seuls frais :

a) immédiatement (et 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) aient eu connaissance d'un incident de sécurité des informations) signalent un tel incident de sécurité des informations au Centre de sécurité des clients, qui fonctionne 24h/24 et 7j/7 et peut être joint au +41 21 924 91 91 ou gsoc@nestle.com, résumant de manière raisonnablement détaillée l'effet sur le Client et ses Affiliés, s'ils sont connus ;

b) enquêter (avec la participation du client et/ou d'un tiers enquêteur judiciaire indépendant) sur un tel incident de sécurité des informations, effectuer une évaluation des risques et élaborer un plan de mesures correctives ;

c) fournir au client un rapport écrit sur cette évaluation des risques, y compris une analyse juridique, afin de déterminer la conformité avec toutes les lois applicables et le plan d'action adopté ou à adopter par le fournisseur ; et

d) préparer et mettre en oeuvre un plan de correction pour prendre toutes les mesures correctives nécessaires et recommandées, et coopérer pleinement avec le Client et tous les Affiliés du Client dans tous les efforts raisonnables et légaux pour prévenir, atténuer, corriger et corriger les effets de l'incident de sécurité des informations.

6.2. Le Fournisseur testera toutes les fonctionnalités de ses procédures de réponse aux incidents de sécurité au moins une fois par année civile et fournira les résultats de ces tests au Client sur demande.

7. Journalisation

7.1. Le fournisseur aura mis en place un programme complet de gestion des registres définissant la portée, la production, la transmission, le stockage, l'analyse et l'élimination des billes en s'appuyant sur la publication spéciale 800-92 de l'Institut national de normalisation et de technologie (NIST) (ou document de remplacement). Les systèmes et les services fourniront des capacités de journalisation conformément aux principes suivants :

a) la portée de l'enregistrement et la politique de conservation seront fondées sur une approche axée sur les risques ;

b) les journaux seront suffisants pour permettre une analyse judiciaire des incidents de sécurité de l'information ;

c) les journaux enregistreront les modifications administratives apportées aux Services ;

d) les registres seront conservés physiquement et virtuellement en lieu sûr afin d'empêcher toute manipulation ;

e) les mots de passe ne seront enregistrés dans aucune circonstance ; et

f) L'intégration de l'API sera disponible pour le transfert des données vers la plate-forme SIEM du client si nécessaire et en accord avec le client.

7.2. Le Fournisseur fera en sorte que ses Affiliés et ses Sous-traitants fournissent au Client des copies de tous les fichiers journaux raisonnablement demandés pour aider à l'analyse ou à l'investigation des incidents de sécurité de l'information.

8. Sécurité physique

Toutes les installations contenant les systèmes devront, au minimum :

a) être conçus de manière structurelle pour résister à des conditions météorologiques défavorables et à d'autres conditions naturelles raisonnablement prévisibles ;

b) avoir des mesures de protection de l'environnement physique appropriées 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 site ; et

d) avoir des contrôles appropriés pour s'assurer que seul le personnel autorisé des fournisseurs est autorisé à accéder physiquement à l'installation.

9. Aliénation des médias

Le fournisseur utilisera les processus normalisés de l'industrie décrits dans la publication spéciale 800-88 (ou document de remplacement) de l'Institut national de normalisation et de technologie (NIST) pour éliminer les médias contenant des données sur le client.

10. Sauvegarde

Le fournisseur :

a) s'assurer que les données du client sont sauvegardées et stockées dans un emplacement et un format disponibles pour la récupération selon les besoins ;

b) sauvegarder des copies des procédures de récupération des données et des données du client dans un endroit différent de celui où se trouve l'équipement informatique principal traitant les données du client ;

c) disposer de procédures spécifiques régissant l'accès aux copies des données clients ;

d) examiner et tester 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 devaient être entrées manuellement dans le processus de récupération des données.

11. Reprise après sinistre

11.1. Le fournisseur a et maintiendra un plan de reprise après sinistre, de continuité des opérations et d'urgence approprié ainsi que les politiques et procédures connexes (collectivement, le "plan de reprise après sinistre"). Le plan de reprise après sinistre sera examiné par le fournisseur chaque année ou lorsqu'un changement important se produit, et permettra de poursuivre l'exploitation en cas d'événement catastrophique affectant les opérations commerciales du fournisseur sans réduction ou dégradation substantielle de la fonctionnalité ou de la disponibilité.

11.2. Le fournisseur teste toutes les fonctionnalités de son plan de reprise après sinistre au moins une fois par année civile et fournit les résultats de ces tests au client sur demande.

11.3. 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 cette erreur et corrigera cette erreur à ses propres frais et suivra sa procédure de reprise après sinistre. En cas d'erreurs de traitement causées par le Client ou un tiers (à l'exclusion du Sous-traitant du Fournisseur), le Fournisseur corrigera ces erreurs sur avis écrit du Client et à ses frais raisonnables.

12. Logiciels malveillants

12.1. Le Fournisseur fera en sorte que ses Affiliés et ses Sous-traitants : a) installent et maintiennent un logiciel anti-malware standard et, dans la mesure du possible, utilisent des fonctionnalités de protection en temps réel et b) maintiennent le logiciel anti-malware conformément aux pratiques recommandées par le fournisseur de logiciel anti-malware afin d'empêcher les Systèmes et/ou les Services d'être infectés ou affectés par la présence de Code Malveillant.

12.2. Fournisseur s'assure que le logiciel anti-malware utilisé par Fournisseur et ses affiliés et sous-traitants vérifieront les nouvelles mises à jour de logiciels malveillants au moins une fois par jour et que les signatures anti-malware associées sont à jour.

12.3. Le Fournisseur va, et fera en sorte que ses Affiliés et ses Sous-traitants, retirent immédiatement tout Code Malveillant découvert ou qui pourrait être présent dans les Systèmes ou les Services.

12.4. Le fournisseur effectuera une analyse en temps réel des fichiers et autres données téléchargés dans les Services afin d'identifier et d'éliminer les fichiers ou autres données contenant du code malveillant.

12.5. Le Fournisseur s'assure que les Services n'introduiront, n'autoriseront ni ne faciliteront l'introduction dans un Système de tout Code Malveillant.

13. Chiffrement des données

13.1. Le fournisseur fera en sorte que ses affiliés et ses sous-traitants mettent en oeuvre et utilisent les produits de chiffrement acceptés dans la publication spéciale NIST 800-52 (ou document de remplacement) pour protéger les données client (y compris les informations d'identification) lors des transmissions sur les réseaux publics.

13.2. Lorsque le Client en a convenu par écrit, le Fournisseur fera en sorte que ses Affiliés et ses Sous-traitants mettent en oeuvre et utilisent les produits de cryptage acceptés dans la Publication spéciale 800-52 (ou document de remplacement) de la NIST pour protéger les Données du Client (y compris les informations d'identification) lors des transmissions sur des réseaux privés.

13.3. Si le Client en a convenu par écrit, les Données du Client inactives, y compris toute sauvegarde des Données du Client, seront cryptées à l'aide d'algorithmes de cryptage approuvés par la Publication 140 des Normes fédérales de traitement de l'information (FIPS PUB 140 ou document remplaçant).

14. Accès aux données

Le fournisseur s'assure que toute personne ayant accès aux données du client dans les installations du fournisseur ou des sociétés affiliées du fournisseur ou des sous-traitants aura accès aux données du client uniquement en fonction d'une approche/d'un besoin de savoir moins privilégiés. Le fournisseur garantit que les données client seront toujours protégées lorsqu'elles sont transférées vers des environnements non actifs en anonymisant/masquant les données client.

15. Propriété et séparation des données client

15.1. Les Données Client sont et resteront la propriété exclusive du Client.

15.2. Le Fournisseur s'assure que toutes les données mises à la disposition du Fournisseur par le Client ou l'un de ses Affiliés ou Sous-traitants seront, par des moyens techniques appropriés, logiquement séparées des données du Fournisseur et des données de tout autre client du Fournisseur ou de ses Affiliés ou Sous-traitants.

16. Gestion des vulnérabilités

16.1. Le fournisseur aura mis en place et révisera chaque année ou, lorsqu'un changement important se produit, un programme complet de gestion des vulnérabilités pour l'identification, la catégorisation et la correction en temps opportun des vulnérabilités techniques et des processus aux niveaux de l'infrastructure et des applications du ou des systèmes. Le programme de gestion

des vulnérabilités sera fondé sur la publication spéciale 800-40 du NIST (ou document remplaçant).

16.2. Le fournisseur fera tout son possible pour s'assurer que les correctifs logiciels pour corriger les vulnérabilités sont installés et activés dans les délais suivants :

16.3. 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 Système commun de notation des vulnérabilités (SVAC) fourni par le Forum des équipes d'intervention et de sécurité en cas d'incident (FIRST).

17. Connexion à distance

Lorsque le Fournisseur se connecte à distance au réseau du Client et/ou accède à distance aux systèmes privés ou publics 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 les accès aux systèmes d'information du Client sont consignés et peuvent être surveillés ;

b) la connexion réseau est uniquement un moyen de partager certaines données entre le Fournisseur et le Client et de faciliter l'exécution des services du Fournisseur au Client ;

c) Le Fournisseur est responsable de toutes les données et/ou modifications postées par ou pour le compte du Fournisseur, et le Client ne sera pas responsable, ni n'aura aucune obligation de surveiller ou de maintenir une surveillance, en ce qui concerne ces modifications ou ces données ;

d) Le client ne garantit pas que l'accès au réseau est sécurisé ;

e) 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

f) lorsque les informations d'identification sont attribuées par le Client aux utilisateurs autorisés du Fournisseur, ces informations d'identification sont confidentielles et personnelles pour chaque utilisateur et ne peuvent être divulguées ou partagées pour quelque raison que ce soit.