Exigences en matière de sécurité des informations

1. Introduction

Le Fournisseur et CWT ont conclu un accord en vertu duquel le Fournisseur a accepté de fournir des services et/ou des produits selon les termes de cet accord (« **Accord** »). Le Fournisseur s'engage à se conformer et à faire en sorte que les Tiers agissant en son nom se conforment aux exigences de sécurité de l'information contenues dans le présent document (« **Exigences de sécurité de l'information ») ** et aux mesures de sécurité de l'information requises (« **Mesures de sécurité techniques et organisationnelles** »). Les exigences de sécurité de l'information et les mesures de sécurité techniques et organisationnelles sont incorporées et font partie intégrante de l'accord.

2. Définitions

2.1 Sauf indication contraire ou développement dans les présentes, les termes définis auront la même signification que celle indiquée dans le Contrat. Les termes définis suivants s'appliquent aux présentes exigences de sécurité de l'information . En cas de conflit entre la définition contenue dans l'Accord et celles des présentes, la définition du présent document prévaudra en ce qui concerne les exigences de sécurité de l'information.

« **Affiliés** », sauf définition contraire dans le Contrat, désigne, en référence à une partie, toute société ou autre entité juridique qui, à la date de signature du Contrat, directement ou indirectement (i) contrôle une partie ; ou (ii) est contrôlée, par une partie ; ou (iii) est contrôlée par une société ou une entité qui contrôle directement ou indirectement une partie. À ces fins, « contrôle » désigne le droit d'exercer plus de cinquante pour cent (50 %) des droits de vote ou un droit de propriété similaire ; mais seulement aussi longtemps que ce contrôle continuera d'exister.

« Employé autorisé » désigne les employés du fournisseur qui ont besoin de connaître ou d' accéder autrement aux informations confidentielles et aux informations personnelles pour permettre au fournisseur de s'acquitter de ses obligations en vertu du contrat.

« **Partie autorisée » ou « Parties autorisées** » désigne les (i) Employés autorisés du Fournisseur ; et (ii) des tiers qui ont besoin de connaître ou d'accéder autrement aux informations personnelles et aux informations confidentielles pour permettre au fournisseur de s'acquitter de ses obligations en vertu du contrat, et qui sont liés par écrit par la confidentialité et d'autres obligations suffisantes pour protéger les informations personnelles et les informations confidentielles. conformément aux termes et conditions de l' accord et du présent document.

« Informations confidentielles » désigne toute information commercialement sensible, exclusive ou autrement confidentielle concernant (a) CWT, ses partenaires et ses Sociétés affiliées ; (b) un client de CWT et les employés, sous-traitants, sous-traitants ou fournisseurs d'un client de CWT ; (c) le personnel de CWT ; (d) ses partenaires indépendants et coentrepreneurs ; ou (e) le contenu et/ou l'objet du Contrat, qu'il soit oral, écrit ou qui, par tout autre moyen, pourrait entrer directement ou indirectement en la possession du Vendeur

ou en la possession des Parties autorisées à la suite de ou en relation avec le Accord. Pour éviter toute ambiguïté, tous les produits du travail constituent des informations confidentielles.

« **CWT** », sauf indication contraire dans le Contrat, désigne l'entité CWT décrite dans le Contrat ainsi que ses Affiliés.

« **Zone démilitarisée** » ou « **DMZ** » est un réseau ou un sous-réseau situé entre un réseau interne de confiance, tel qu'un réseau local (LAN) privé d'entreprise, et un réseau externe non fiable, tel que l'Internet public. Une DMZ permet d'empêcher les utilisateurs externes d'accéder directement aux systèmes internes et à d'autres ressources.

« Processus de gestion des incidents » est un processus et une procédure documentés développés par le fournisseur à suivre en cas d'attaque réelle ou suspectée, d'intrusion, d'accès non autorisé, de perte ou de toute autre violation impliquant la confidentialité, la disponibilité ou l'intégrité. des renseignements personnels et des renseignements confidentiels de CWT.

« masquage » est le processus de couverture des informations affichées sur un écran.

« Appareils mobiles et portables » désigne les ordinateurs, appareils, supports et systèmes mobiles et/ou portables pouvant être facilement transportés, déplacés, transportés ou transportés qui sont utilisés dans le cadre du Contrat. Des exemples de tels appareils incluent les ordinateurs portables, les tablettes, les disques durs USB, les clés USB, les assistants numériques personnels (PDA), les téléphones portables ou de données, et tout autre appareil sans fil, périphérique ou amovible avec la capacité de stocker des informations confidentielles et des informations personnelles. .

« **Informations personnelles** », sauf définition contraire dans l'Accord, telles que définies dans le règlement (UE) 2016/679 et d'autres lois mondiales applicables en matière de sécurité de l'information, de protection des données et de confidentialité, désigne toute information relative à une personne physique identifiée ou identifiable, qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Les renseignements personnels appartiennent à CWT, et non au fournisseur.

« **Security Gateway »** désigne un ensemble de mécanismes de contrôle entre deux ou plusieurs réseaux ayant différents niveaux de confiance qui filtrent et consignent le trafic passant, ou tentant de passer, entre les réseaux, et les serveurs d'administration et de gestion associés. Les exemples de passerelles de sécurité incluent les pare-feu, les serveurs de gestion de pare-feu, les hop boxes, les contrôleurs de session en bordure, les serveurs proxy et les dispositifs de prévention des intrusions.

« Authentification forte » signifie l'utilisation de mécanismes d'authentification et de méthodologies d'authentification qui nécessitent plusieurs facteurs d'authentification, y

compris au moins deux des éléments suivants : (1) Connaissance - quelque chose que l'utilisateur connaît, par exemple un mot de passe ou un numéro d'identification personnel, (2) Propriété - quelque chose l'utilisateur possède, par exemple, un jeton, une carte à puce, un téléphone mobile, et (3) Inhérence - quelque chose que l'utilisateur est, par exemple une empreinte digitale.

« Chiffrement fort » signifie l'utilisation de technologies de chiffrement avec des longueurs de clé minimales de 256 bits pour le chiffrement symétrique et de 1024 bits pour le chiffrement asymétrique dont la force fournit une assurance raisonnable qu'elle protégera les informations chiffrées contre tout accès non autorisé et est adéquate pour protéger la confidentialité. et la confidentialité des informations cryptées , et qui intègre une politique documentée pour la gestion des clés de cryptage et des processus associés adéquats pour protéger la confidentialité et la confidentialité des clés et des mots de passe utilisés comme entrées de l'algorithme de cryptage. Le cryptage fort comprend, mais sans s'y limiter : SSL v3.0+/TLS v1.2, protocole de tunnellisation point à point (PPTP), AES 256, FIPS 140-2 (gouvernement des États-Unis uniquement), RSA 1024 bits, SHA1/SHA2 /SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 ou WPA2.

« **Mesures de sécurité techniques et organisationnelles** » désigne toutes les activités requises en vertu des présentes exigences de sécurité de l'information pour accéder, gérer, transférer, traiter, stocker, conserver et détruire des informations ou des données ; divulguer et notifier les parties concernées conformément à l'Accord et aux lois applicables en matière de confidentialité des informations et de protection des données ; et pour protéger les informations ou les données afin d'assurer la disponibilité, l'intégrité, la confidentialité et la confidentialité, ou informer les personnes de tout manquement à la protection de ces informations ou données. Les mesures comprennent, mais sans s'y limiter, celles requises ou interprétées comme étant requises en vertu du règlement général sur la protection des données (RGPD) de l'UE, de la directive sur les services de paiement de l'UE, du California Consumer Privacy Act, du NYS DFS 23 NYCRR 500 , du Gramm-Leach Bliley Act des États-Unis (GLBA), la Health Insurance Portability and Accountability Act (HIPAA) des États-Unis, les exigences de l'UE/Suisse en matière de confidentialité des données et toute autre loi internationale et américaine, interprétations juridiques officielles ou précédents concernant des informations ou des données dans le cadre de l'Accord .

« **Tiers »** ou « **Tiers** » signifie Vendeur les sous-traitants , les consultants, le personnel temporaire, les sous-traitants ou les fournisseurs et/ou agents supplémentaires agissant au nom du fournisseur et incluent toute définition de tiers en vertu de la législation européenne, américaine ou internationale applicable.

« **Vendeur** » désigne l'entité contractante indiquée dans le Contrat, ainsi que ses Sociétés affiliées et ses Tiers.

3 . <u>Organisation de la sécurité de l'information</u>

Le vendeur doit , au minimum :

3.1 Assurez-vous que seules les parties autorisées ont accès aux informations personnelles et aux informations confidentielles.

3.2 Mettre en œuvre des mesures de sécurité techniques et organisationnelles qui ne sont pas moins rigoureuses que les meilleures pratiques de sécurité de l'information pour protéger l'intégrité, la disponibilité et la confidentialité des informations confidentielles, des informations personnelles et d'autres informations non publiques et empêcher l'accès, l'acquisition, la divulgation, la destruction et l'altération non autorisés. , la perte accidentelle, la mauvaise utilisation ou l'endommagement des informations personnelles ou des informations confidentielles.

3.3 Établir, mettre en œuvre et maintenir, conformément aux meilleures pratiques de l'industrie , des politiques et un programme de mesures de sécurité organisationnelles, opérationnelles, administratives, physiques et techniques et organisationnelles appropriées pour (1) empêcher tout accès par des parties non autorisées aux informations personnelles et aux informations confidentielles dans d'une manière non autorisée par l' Accord ou les présentes Exigences de sécurité de l'information, et (2) se conformer à toutes les lois et réglementations applicables et aux normes industrielles applicables.

3.4 Fournir aux parties autorisées qui auront accès aux informations personnelles et aux informations confidentielles une supervision, des conseils et une formation sur les mesures de sécurité techniques et organisationnelles, y compris une formation qui propose des exercices pratiques alignés sur les scénarios de menace actuels et fournit des commentaires aux personnes qui suivent la formation . Le fournisseur doit fournir une formation sur les mesures de sécurité techniques et organisationnelles lors de l' embauche d'un employé autorisé et avant l'accès d'une partie autorisée aux informations confidentielles et aux informations personnelles. Une formation de recyclage doit être dispensée au moins une fois par an et dès que possible après tout changement important dans les mesures de sécurité techniques et organisationnelles du fournisseur.

3.5 Fournir une formation spécialisée spécifique aux Parties autorisées ayant des fonctions de sécurité importantes, y compris, mais sans s'y limiter, les ressources humaines ou les fonctions de technologie de l'information, et toute fonction d'administrateur de technologie. Au minimum, la formation spécialisée doit inclure, selon le rôle, les procédures de sécurité de l'information, l'utilisation acceptable des ressources de sécurité de l'information, les menaces actuelles contre les systèmes d'information, les fonctionnalités de sécurité de systèmes spécifiques et les procédures d'accès sécurisé.

3.6 Prendre des mesures raisonnables pour empêcher l'accès non autorisé ou la perte d'informations personnelles et d'informations confidentielles et des services, systèmes, appareils ou supports contenant ces informations.

3.7 Utiliser des processus et des procédures d'évaluation des risques pour évaluer régulièrement les systèmes utilisés pour fournir des services ou des produits à CWT. Le fournisseur doit remédier à ces risques dès que raisonnablement possible et en fonction du niveau de risque pour les informations personnelles et les informations confidentielles compte tenu des

menaces connues au moment de l'identification. Exploiter un processus permettant de signaler les risques ou les incidents suspectés à l'équipe de sécurité du fournisseur.

3.8 Dans la mesure où le Fournisseur fournit des services conformément au Contrat dans les installations de CWT ou en utilisant des services, des systèmes, des appareils ou des supports détenus, exploités ou gérés par CWT, le Fournisseur doit faire en sorte que toutes les Parties autorisées se conforment à toutes les politiques de CWT mises à la disposition du Fournisseur , à sa demande, applicables à cet accès. Le Fournisseur doit aviser CWT rapidement par écrit lorsqu'une Partie autorisée n'a plus besoin d'accéder aux Informations personnelles ou aux Informations confidentielles pour que le Fournisseur fournisse des produits ou des services à CWT , y compris, sans s'y limiter , lorsqu'une Partie autorisée est licenciée ou n'est plus en activité . services en vertu de l'Accord.

3.9 Tenir des registres des parties autorisées et des ressources du fournisseur qui accèdent, transfèrent, conservent, stockent ou traitent les informations personnelles et les informations confidentielles.

3.10 Effectuer des vérifications complètes des antécédents de toutes les parties autorisées avant l'embauche, dans la mesure permise par la loi . La vérification complète des antécédents des personnes doit inclure , au minimum, les antécédents professionnels de la personne, son casier judiciaire, ses antécédents de crédit, ses références et toute autre exigence de vérification des antécédents standard de l'industrie.

3.11 Disposer d'un ou plusieurs membres du personnel qualifiés chargés de maintenir son programme de sécurité de l'information et doit rendre compte de son programme de sécurité de l'information au moins une fois par an au conseil d'administration du Fournisseur ou à un organe directeur équivalent. Le fournisseur doit s'assurer que son personnel de sécurité possède une expérience et une formation raisonnables et nécessaires en matière de sécurité de l'information, y compris le maintien des connaissances sur l'évolution des menaces et des contre-mesures. Sur demande, le Fournisseur fournira à CWT un point de contact pour tous les éléments liés à la sécurité des informations.

3.12 Exiger des engagements contractuels de non-divulgation ou de confidentialité des Parties autorisées avant de leur donner accès aux Informations personnelles et aux Informations confidentielles.

3.13 Veiller à ce que toutes les parties autorisées qui peuvent effectuer des travaux dans le cadre de l'accord ou qui peuvent avoir accès à des informations personnelles ou à des informations confidentielles respectent ces mesures de sécurité techniques et organisationnelles, qui doivent être attestées par un accord écrit non moins restrictif que ces exigences de sécurité de l'information. .

4. Sécurité physique et environnementale

Le vendeur doit , au minimum :

4.1 Assurez-vous que tous les systèmes et autres ressources du Fournisseur destinés à être utilisés par plusieurs utilisateurs sont situés dans des installations physiques sécurisées avec un accès limité et réservé aux personnes autorisées uniquement.

4.2 Surveiller et enregistrer, à des fins d'audit, l'accès aux installations physiques contenant des systèmes et d'autres ressources destinées à être utilisées par plusieurs utilisateurs dans le cadre de l'exécution par le Fournisseur de ses obligations en vertu du Contrat.

4.3 Exiger que toutes les parties autorisées respectent une politique de bureau propre et verrouillent les écrans des postes de travail avant de quitter les zones de travail.

4.4 Récupérez tous les actifs de l'entreprise lors de la cessation d'emploi ou de la résiliation du contrat.

4.5 Limiter et surveiller l'accès physique à ses installations selon les exigences suivantes :

a. L'accès des visiteurs est consigné, qui est conservé pendant trois (3) mois comprenant le nom du visiteur, la société qu'il représente et le nom de l'employé autorisant l'accès physique. Les visiteurs doivent être escortés par un employé du fournisseur en tout temps.
b. L'accès est limité au personnel approprié, sur la base d'un besoin de savoir.
c. Tous les employés doivent porter un badge nominatif fourni par l'entreprise et tous les visiteurs ou tiers doivent porter un badge d'invité/visiteur fourni par l'entreprise.
d. L'accès est révoqué immédiatement après la résiliation du personnel du Fournisseur ou du Tiers , et tous les mécanismes d'accès physiques, tels que les clés, les cartes d'accès, etc., sont restitués ou désactivés.
e. Le centre de données ou la salle informatique est verrouillé et l'accès est limité à ceux qui en ont besoin pour effectuer leurs tâches professionnelles.
f. Lorsque la loi l'autorise, utilisez des caméras vidéo pour surveiller l'accès physique individuel aux zones sensibles et examinez régulièrement ces données. Les séquences vidéo doivent être conservées pendant au moins trois (3) mois.
g. L'équipement utilisé pour stocker, traiter ou transmettre des informations personnelles et des informations confidentielles doit être physiquement sécurisé, y compris les points d'accès sans fil, les passerelles, les appareils portables, le matériel de réseau/communication et les lignes de télécommunication.

4.6 Mettez en place des contrôles pour minimiser les risques et vous protéger contre les menaces physiques.

4.7 Maintenir tous les actifs matériels traitant ou manipulant les informations personnelles et les informations confidentielles conformément aux exigences de maintenance recommandées par le fabricant .

4.8 réseaux accessibles au public et les prises réseau logiquement et physiquement du réseau interne du fournisseur et limités uniquement aux utilisateurs authentifiés ou désactivés par défaut.

4.9 Protégez tout appareil qui capture des données de carte de paiement via une interaction physique directe contre la falsification et la substitution en inspectant périodiquement les surfaces de l'appareil pour détecter toute falsification ou substitution ; fournir une formation au personnel pour qu'il soit conscient des tentatives d'altération ou de remplacement d'appareils.

4.10 Contrôlez et séparez les points d'accès tels que les zones de livraison et de chargement et les autres points de tous les centres d'accès, de gestion, de stockage ou de traitement des informations personnelles et des informations confidentielles.

4.11 Assurez-vous que les centres de données du fournisseur disposent de dispositifs de chauffage, de refroidissement, d'extinction d'incendie, de détection d'eau et de détection de chaleur/fumée. Les centres de données et les salles informatiques des fournisseurs doivent être exempts de matériaux combustibles (par exemple , boîtes, papier, etc.) ou stockés dans des armoires métalliques.

5. Contrôle d'accès

Le vendeur doit , au minimum :

5.1 Prendre toutes les mesures raisonnables pour empêcher toute personne autre que les Parties autorisées d'accéder aux Informations personnelles et aux Informations confidentielles de quelque manière ou à toute fin non autorisées par CWT et le Contrat.

5.2 Séparez les informations de CWT des données des autres clients du Fournisseur ou des propres applications et informations du Fournisseur, soit en utilisant des serveurs physiquement séparés, soit en utilisant des contrôles d'accès logiques lorsque la séparation physique des serveurs n'est pas mise en œuvre.

5.3 Identifier et exiger que les propriétaires appropriés examinent et approuvent l'accès aux systèmes utilisés pour accéder, traiter, gérer ou stocker les informations personnelles et les informations confidentielles au moins une fois par trimestre afin de supprimer tout accès non autorisé ; et maintenir et suivre les approbations d'accès.

5.4 Supprimer l'accès aux systèmes gérant les informations personnelles et les informations confidentielles dans les 24 heures suivant la fin de la relation entre la partie autorisée et le fournisseur ; et maintenir des procédures raisonnables pour supprimer l'accès à ces systèmes dans les trois jours ouvrables lorsqu'il n'est plus nécessaire ou pertinent pour l'exercice de leurs fonctions . Tous les autres identifiants d'utilisateur doivent être désactivés ou supprimés après 90 jours calendaires d'inactivité.

5.5 Limitez l'accès de l'administrateur système (également appelé root, privilégié ou super utilisateur) aux systèmes d'exploitation destinés à être utilisés par plusieurs utilisateurs uniquement aux personnes nécessitant un tel accès de haut niveau dans l'exécution de leur travail. Utilisez des identifiants d'administrateur système de paiement avec des identifiants

de connexion utilisateur individuels et des journaux d'activité pour gérer un accès hautement sécurisé et réduire l'accès de haut niveau à un nombre très limité d'utilisateurs. Exiger des administrateurs d'application, de base de données, de réseau et de système qu'ils limitent l'accès des utilisateurs aux seules commandes, données, systèmes et autres ressources dont ils ont besoin pour exécuter les fonctions autorisées. Les rôles administratifs du système et les listes d'accès doivent être révisés au moins une fois par an.

5.6 Appliquer la règle du moindre privilège (c.-à-d ., limiter l'accès aux seules commandes, informations, systèmes et autres ressources nécessaires pour exécuter les fonctions autorisées en fonction de la fonction).

5.7 Exigez une authentification forte pour tous les accès administratifs non console , tout accès à distance et tous les accès administratifs aux environnements cloud .

5.8 Interdire et utiliser des mesures de sécurité techniques et organisationnelles pour s'assurer que les informations personnelles ne peuvent pas copier, déplacer ou stocker des informations personnelles sur des disques durs locaux ou couper et coller ou imprimer des informations personnelles.

5.9 Activez l'utilisation des fonctionnalités d'accès à distance uniquement lorsque cela est nécessaire, surveillez-les pendant leur utilisation et désactivez-les immédiatement après utilisation.

5.10 Exiger une authentification forte pour se connecter aux ressources internes du fournisseur contenant des informations personnelles et des informations confidentielles.

6. <u>Identification et authentification</u>

Le vendeur doit , au minimum :

6.1 Attribuez des ID utilisateur uniques à des utilisateurs individuels et attribuez des mécanismes d'authentification à chaque compte individuel.

6.2 Utiliser un processus documenté de gestion du cycle de vie de l'ID utilisateur, y compris, mais sans s'y limiter, les procédures de création de compte approuvée, de suppression de compte en temps opportun et de modification de compte (par exemple, modifications des privilèges, étendue d'accès, fonctions/rôles) pour tout accès aux informations personnelles et Informations confidentielles et dans tous les environnements (par exemple, production, test, développement, etc.). Ce processus doit inclure un examen des privilèges d'accès et de la validité du compte à effectuer au moins une fois par trimestre.

6.3 Restreignez tout accès aux informations personnelles et aux informations confidentielles à ceux qui utilisent un identifiant et un mot de passe valides, et exigez que les identifiants d'utilisateur uniques utilisent l'un des éléments suivants : mot de passe ou phrase de passe, authentification à deux facteurs ou valeur biométrique.

6.4 Exiger un mot de passe complexe et répondre aux exigences de construction de mot de passe suivantes : un minimum de douze (12) caractères pour les mots de passe système et quatre (4) caractères pour les codes d'accès des tablettes et des smartphones. Les mots de passe système doivent contenir trois (3) des éléments suivants : majuscules, minuscules, chiffres ou caractères spéciaux. Les mots de passe ne doivent pas non plus être identiques à l'ID utilisateur auquel ils sont associés, contenir un mot du dictionnaire, des numéros séquentiels ou répétés, et ne pas être l'un des 24 derniers mots de passe. Exiger l'expiration du mot de passe à intervalles réguliers ne dépassant pas quatre-vingt-dix (90) jours. Masquez tous les mots de passe lorsqu'ils sont affichés.

6.5 Limitez les tentatives de connexion infructueuses à un maximum de cinq (5) tentatives de connexion infructueuses dans les 24 heures et verrouillez le compte d'utilisateur lorsque cette limite est atteinte dans un état persistant. L'accès au compte utilisateur peut être réactivé ultérieurement par un processus manuel nécessitant la vérification de l'identité de l'utilisateur.

6.6 Vérifiez l'identité de l'utilisateur et définissez un usage unique et réinitialisez les mots de passe à une valeur unique pour chaque utilisateur. Changement rapide systématiquement après la première utilisation.

6.7 Utilisez une méthode sécurisée pour transmettre les justificatifs d'authentification (par exemple, les mots de passe) et les mécanismes d'authentification (par exemple, les jetons ou les cartes à puce).

6.8 Limitez les mots de passe de compte de service et de proxy à un minimum de 20 caractères , y compris des caractères majuscules, minuscules et numériques, ainsi que des symboles spéciaux. Modifiez les mots de passe du compte de service et du proxy au moins une fois par an et après la cessation d'emploi de toute personne connaissant le mot de passe.

6.9 Mettre fin aux sessions interactives ou activer un économiseur d'écran sécurisé et verrouillable nécessitant une authentification, après une période d'inactivité ne dépassant pas quinze (15) minutes.

6.10 Utilisez une méthode d'authentification basée sur la sensibilité des informations personnelles et des informations confidentielles. Chaque fois que les identifiants d'authentification sont stockés, le fournisseur doit les protéger à l'aide d'un cryptage fort.

6.11 Configurez les systèmes pour qu'ils expirent automatiquement après une période d'inactivité maximale comme suit : serveur (15 minutes), poste de travail (15 minutes), appareil mobile (4 heures), protocole de configuration d'hôte dynamique (7 jours), réseau privé virtuel (24 heures).

7. Acquisition, développement et maintenance des systèmes d'information

Le vendeur doit , au minimum :

7.1 Afficher une bannière d'avertissement sur les écrans ou les pages de connexion comme spécifié par écrit par CWT pour les produits ou services de la marque CWT ou pour les produits et logiciels développés pour CWT.

7.2 Renvoyez tous les dispositifs d'accès appartenant à ou fournis par CWT dès que possible, mais en aucun cas plus de quinze (15) jours après le plus proche des événements suivants :

a. l'expiration ou la résiliation du Contrat ;
b. la demande de CWT pour la restitution de ces biens ; ou
c. la date à laquelle le Fournisseur n'a plus besoin de ces appareils.

7.3 Utiliser une méthodologie de gestion des applications efficace qui intègre des mesures de sécurité techniques et organisationnelles dans le processus de développement de logiciels et s'assurer que les mesures de sécurité techniques et organisationnelles, telles que représentées par les meilleures pratiques de l'industrie, sont mises en œuvre par le fournisseur en temps opportun.

7.4 Suivez les procédures de développement standard de l' industrie , y compris la séparation de l'accès et du code entre les environnements de non-production et de production et la séparation des tâches associées entre ces environnements.

7.5 S'assurer que les contrôles internes de sécurité des informations pour le développement de logiciels sont évalués régulièrement et reflètent les meilleures pratiques de l'industrie, et réviser et mettre en œuvre ces contrôles en temps opportun.

7.6 Gérer la sécurité du processus de développement et s'assurer que des pratiques de codage sécurisées sont mises en œuvre et suivies, y compris des contrôles cryptographiques appropriés, des protections contre les codes malveillants et un processus d'examen par les pairs.

7.7 Effectuez des tests d'intrusion sur des applications fonctionnellement complètes avant leur mise en production et par la suite, au moins une fois par an et après toute modification importante du code source ou de la configuration conforme à OWASP, CERT, SANS Top 25 et PCI-DSS. Corrigez toutes les vulnérabilités exploitables avant le déploiement dans l'environnement de production.

7.8 Utilisez des données anonymisées ou obscurcies dans des environnements hors production. N'utilisez jamais de données de production en texte brut dans un environnement de non-production et n'utilisez jamais d'informations personnelles dans des environnements de non-production pour quelque raison que ce soit. Assurez-vous que toutes les données de test et tous les comptes sont supprimés avant la mise en production.

7.9 Examinez le code source ouvert ou gratuit approuvé par CWT, les logiciels, les applications ou les services pour détecter les défauts, les bogues, les problèmes de sécurité ou le non-respect des conditions de licence de source ouverte ou gratuite. Le Fournisseur doit informer CWT à

l'avance de l'utilisation de tout code source ouvert ou gratuit et, si l'utilisation est approuvée par CWT, fournir à CWT le nom, la version et l'URL du code source ouvert ou gratuit. Le Fournisseur déclare et garantit que (a) tout code source ouvert ou gratuit qu'il utilise dans ses produits ou services sera concédé sous licence de code source ouvert ou libre "permissif" et non sous licence restrictive, réciproque, héréditaire ou copyleft ; (b) Le fournisseur a le droit de modifier, d'adapter librement le code source ouvert ou gratuit et de combiner le code source ouvert ou gratuit ou de contenir du code source ouvert ou gratuit avec du code propriétaire sans imposer de restrictions sur ces modifications, adaptations ou combinaisons ou code propriétaire qui contient code source ouvert ou libre et comment ceux-ci peuvent être concédés sous licence (collectivement, les « **œuvres dérivées** ») et (c) ces œuvres dérivées ne seront soumises à aucune licence de source ouverte ou gratuite nécessitant une licence pour l'œuvre dérivée ou la rendant disponible gratuitement à des tiers dans le cadre des conditions de licence open source ou libre.

7.10 Ne partager aucun code créé dans le cadre de l'Accord, quel que soit le stade de développement, dans un environnement partagé ou non privé, tel qu'un référentiel de code d'accès ouvert, quelle que soit la protection par mot de passe.

8. Intégrité des logiciels et des données

Le vendeur doit , au minimum :

8.1 Dans les environnements où un logiciel antivirus est disponible dans le commerce, ayez un logiciel antivirus à jour installé et en cours d'exécution pour rechercher et supprimer rapidement ou mettre en quarantaine les virus et autres logiciels malveillants de tout système ou appareil.

8.2 Séparez les informations et ressources hors production des informations et ressources de production.

8.3 Assurez-vous que les équipes utilisent un processus de contrôle des modifications documenté pour toutes les modifications du système, y compris les procédures de retrait pour tous les environnements de production et les processus de modification d'urgence. Inclure les tests, la documentation et les approbations pour toutes les modifications du système et exiger l'approbation de la direction pour les modifications importantes de ces processus.

8.4 Construire et maintenir une zone PCI si le fournisseur traite ou stocke les données du titulaire de la carte.

8.5 Pour les applications qui utilisent une base de données qui autorise les modifications des informations personnelles et des informations confidentielles, activez et maintenez les fonctionnalités de journalisation d'audit des transactions de la base de données qui conservent les journaux d'audit des transactions de la base de données pendant au moins un (1) an avec trois mois immédiatement disponibles pour analyse.

8.6 Examinez le logiciel pour trouver et corriger les vulnérabilités de sécurité lors de la mise en œuvre initiale et lors de toute modification et mise à jour importantes.

8.7 Effectuer des tests d'assurance qualité pour les composants de sécurité (par exemple, tests des fonctions d'identification, d'authentification et d'autorisation), ainsi que toute autre activité conçue pour valider l'architecture de sécurité, lors de la mise en œuvre initiale et lors de toute modification et mise à jour importantes.

9. <u>Sécurité du système</u>

Le vendeur doit , au minimum :

9.1 Créer et mettre à jour régulièrement les versions les plus récentes des diagrammes de flux de données et de système utilisés pour accéder, traiter, gérer ou stocker les informations personnelles et les informations confidentielles.

9.2 Surveiller activement les ressources de l'industrie (par exemple , , www.cert.org et les listes de diffusion et sites Web des fournisseurs de logiciels pertinents) pour une notification en temps opportun de toutes les alertes de sécurité applicables concernant les systèmes du fournisseur et d'autres ressources d'information.

9.3 Gérez efficacement les clés cryptographiques en réduisant l'accès aux clés au plus petit nombre de dépositaires nécessaires, en stockant les clés cryptographiques secrètes et privées en les chiffrant avec une clé au moins aussi forte que la clé de chiffrement des données et en les stockant séparément de la clé de chiffrement des données dans un environnement sécurisé. dispositif cryptographique, dans le moins d'endroits possible. Changez les clés cryptographiques par défaut lors de l'installation et au moins tous les deux ans, et éliminez les anciennes clés en toute sécurité.

9.4 Analyser les systèmes externes et internes et autres ressources d'information, y compris, mais sans s'y limiter, les réseaux, les serveurs, les applications et les bases de données, avec un logiciel d'analyse des vulnérabilités de sécurité standard applicable pour découvrir les vulnérabilités de sécurité, s'assurer que ces systèmes et autres ressources sont correctement renforcés et identifier tous les réseaux sans fil non autorisés au moins une fois par trimestre et avant la publication des applications et pour les modifications et mises à niveau importantes dans les délais résultant d'analyses de risques basées sur des politiques et normes informatiques raisonnables et généralement acceptées.

9.5 Assurez-vous que tous les systèmes et autres ressources du fournisseur sont et restent renforcés, y compris, mais sans s'y limiter, la suppression ou la désactivation du réseau inutilisé et d'autres services et produits (par exemple, finger, rlogin, ftp et simple Transmission Control Protocol/Internet Protocol (TCP/ IP) services et produits) et l'installation d'un pare-feu système, d'encapsuleurs TCP (Transmission Control Protocol) ou d'une technologie similaire.

9.6 Déployer un ou plusieurs systèmes de détection d'intrusion (IDS), systèmes de prévention d'intrusion (IPS) ou systèmes de détection et de prévention d'intrusion (IDP) dans un mode de fonctionnement actif qui surveille tout le trafic entrant et sortant des systèmes et autres ressources en conjonction avec l'accord de environnements où une telle technologie est disponible dans le commerce et dans la mesure du possible.

9.7 Maintenir un processus d'évaluation des risques pour les résultats de l'évaluation des vulnérabilités aligné sur les meilleures pratiques de l'industrie pour remédier aux vulnérabilités de sécurité dans tout système ou autre ressource, y compris, mais sans s'y limiter, celles découvertes dans les publications de l'industrie, l'analyse des vulnérabilités, l'analyse des virus et l'examen des journaux de sécurité , et appliquez rapidement les correctifs de sécurité appropriés en fonction de la probabilité qu'une telle vulnérabilité puisse être ou soit en train d'être exploitée. Les résultats de l'évaluation des vulnérabilités critiques et les correctifs doivent être corrigés dès leur disponibilité et en aucun cas plus de 7 jours après leur publication. Les résultats des évaluations de vulnérabilité élevée et les correctifs doivent être corrigés dans les 30 jours suivant la publication. Les résultats de l'évaluation de la vulnérabilité moyenne et les correctifs doivent être corrigés dans les 90 jours calendaires. Les résultats de l'évaluation des vulnérabilités faibles et les correctifs doivent être corrigés dans un délai de 120 jours calendaires.

9.8 Effectuer des tests de pénétration du réseau et de la segmentation en interne et en externe au moins une fois par an et après toute mise à niveau ou modification importante de l'infrastructure ou de l'application.

9.9 Supprimer ou désactiver les logiciels non autorisés découverts sur les systèmes du Fournisseur et utiliser des contrôles de logiciels malveillants standard de l'industrie, y compris l'installation, la mise à jour régulière et l'utilisation de routine de produits logiciels anti-malware sur tous les services, systèmes et appareils pouvant être utilisés pour accéder aux informations personnelles et à CWT Information confidentielle. Utilisez un logiciel antivirus fiable et conforme aux meilleures pratiques de l'industrie lorsque cela est possible et assurez-vous que ces définitions de virus restent à jour.

9.10 Maintenir à jour les logiciels de tous les services, systèmes et appareils pouvant être utilisés pour accéder aux Informations personnelles et aux Informations confidentielles de CWT, y compris la maintenance appropriée du ou des systèmes d'exploitation et l'installation réussie de correctifs de sécurité raisonnablement à jour.

9.11 Attribuez des responsabilités d'administration de la sécurité pour la configuration des systèmes d'exploitation hôtes à des personnes spécifiques.

9.12 Modifiez tous les noms de compte par défaut et/ou les mots de passe par défaut.

10. <u>Surveillance</u>

Le vendeur doit , au minimum :

10.1 Conserver les données du journal pour les Informations personnelles et les Informations confidentielles pendant au moins 12 mois à compter de la date de création des données du journal et mettre le journal et ces données à la disposition de CWT dans un délai raisonnable et sur demande, sauf indication contraire dans le Contrat. Les journaux doivent être conçus pour détecter et répondre aux incidents et inclure, mais sans s'y limiter :

a. Tous les accès des utilisateurs individuels aux informations personnelles et aux informations confidentielles
b. Toutes les actions entreprises par ceux qui ont des privilèges administratifs ou root
c. Accès de tous les utilisateurs aux pistes d'audit
d. Tentatives d'accès logique invalides
e. Utilisation et évolution des mécanismes d'identification et d'authentification

10.2 Enregistrer les principales activités système des tiers du fournisseur pour les systèmes contenant des informations personnelles et des informations confidentielles et disposer d'un programme formel d'assurance tierce partie pour s'assurer que les tiers ou les sous-traitants du fournisseur ont mis en place des contrôles de sécurité et des certifications appropriés Faire effectuer une évaluation de la sécurité du cloud si CWT les données résident dans un environnement cloud.

10.3 Limitez l'accès aux journaux de sécurité aux personnes autorisées et protégez les journaux de sécurité contre toute modification non autorisée.

10.4 Mettre en œuvre un mécanisme de détection des modifications (par exemple , surveillance de l'intégrité des fichiers) pour alerter le personnel en cas de modification non autorisée de fichiers système critiques, de fichiers de configuration ou de fichiers de contenu ; configurer le logiciel pour effectuer des comparaisons de fichiers critiques chaque semaine.

10.5 Examinez, au moins une fois par semaine, tous les journaux d'audit de sécurité et liés à la sécurité sur les systèmes contenant des informations personnelles et des informations confidentielles pour détecter les anomalies et documentez et résolvez tous les problèmes de sécurité consignés en temps opportun.

10.6 Examinez quotidiennement tous les événements de sécurité, les journaux des composants du système stockant, traitant ou transmettant les données des titulaires de cartes, les journaux des composants critiques du système et les journaux des serveurs et des composants du système exécutant des fonctions de sécurité.

11. <u>Passerelles de sécurité</u>

Le vendeur doit , au minimum :

11.1 Exiger une authentification forte pour l'accès administratif et/ou de gestion aux passerelles de sécurité, y compris, mais sans s'y limiter, tout accès dans le but d'examiner les fichiers journaux.

11.2 Avoir et utiliser des contrôles, des politiques, des processus et des procédures documentés pour s'assurer que les utilisateurs non autorisés n'ont pas d'accès administratif et/ou de gestion aux passerelles de sécurité, et que les niveaux d'autorisation des utilisateurs pour administrer et gérer les passerelles de sécurité sont appropriés.

11.3 Ayez des contrôles solides autour de la sécurité des e-mails tels que la configuration des protocoles d'authentification DKIM et SPF qui aident à valider qu'un e-mail provient d'une source fiable et validée. Implémentation de DMARC sur les serveurs de messagerie de réception.

11.4 Au moins une fois tous les six (6) mois, assurez-vous que les configurations de Security Gateway sont renforcées en sélectionnant un échantillon de Security Gateways et en vérifiant que chaque ensemble de règles par défaut et ensemble de paramètres de configuration garantit ce qui suit :

un. Le routage source IP (Internet Protocol) est désactivé,
b. L'adresse de bouclage est interdite d'entrer dans le réseau interne,
c. Des filtres anti-spoofing sont mis en place,
ré. Les paquets de diffusion ne sont pas autorisés à entrer dans le réseau,
e. Les redirections ICMP (Internet Control Message Protocol) sont désactivées,
F. Tous les ensembles de règles se terminent par une instruction « DENY ALL », et
g. Chaque règle est traçable à une demande métier spécifique.

11.5 Assurez-vous que les outils de surveillance sont utilisés pour valider que tous les aspects des passerelles de sécurité (par exemple, le matériel, les micrologiciels et les logiciels) sont opérationnels en permanence.

Assurez-vous que toutes les passerelles de sécurité sont configurées et mises en œuvre de manière à ce que toutes les passerelles de sécurité non opérationnelles refusent tout accès.

11.6 Les paquets entrants provenant du réseau externe non approuvé doivent se terminer dans la zone démilitarisée (« **DMZ** ») et ne doivent pas être autorisés à transiter directement vers le réseau interne approuvé. Tous les paquets entrants qui transitent vers le réseau interne de confiance doivent uniquement provenir de la DMZ. La DMZ doit être séparée du réseau externe non approuvé à l'aide d'une passerelle de sécurité et doit être séparée du réseau interne approuvé à l'aide de l'un des éléments suivants :

un. une autre passerelle de sécurité, ou
b. la même passerelle de sécurité utilisée pour séparer la DMZ du réseau externe non approuvé, auquel cas la passerelle de sécurité doit s'assurer que les paquets reçus du réseau externe non approuvé sont immédiatement supprimés ou, s'ils ne sont pas supprimés, sont acheminés uniquement vers la DMZ sans autre traitement de ces paquets entrants ont été exécutés autrement qu'éventuellement en écrivant les paquets dans un journal.

Les éléments suivants doivent uniquement se trouver dans le réseau interne de confiance :

un. Toutes les informations personnelles et les informations confidentielles de CWT stockées sans l'utilisation d'un cryptage fort,
b. La copie officielle des informations
c. Serveurs de bases de données,
ré. Tous les journaux exportés, et
e. Tous les environnements utilisés pour le développement, les tests, le bac à sable, la production et tout autre environnement de ce type ; et toutes les versions de code source.

11.7 Les identifiants d'authentification non protégés par l'utilisation du cryptage fort ne doivent pas se trouver dans la DMZ.

12. <u>Sécurité du réseau</u>

Le vendeur doit , au minimum :

12.1 À la demande de CWT, fournir à CWT un schéma de réseau logique documentant les systèmes et les connexions à d'autres ressources, y compris les routeurs, les commutateurs, les pare-feu, les systèmes IDS, la topologie du réseau, les points de connexion externes, les passerelles, les réseaux sans fil et tout autre appareil devant prendre en charge CWT.

12.2 Maintenez un processus formel pour approuver, tester et documenter toutes les connexions réseau et les modifications apportées aux configurations du pare-feu et du routeur. Configurez les pare-feu pour refuser et consigner les paquets suspects, et restreignez-les pour n'autoriser que le trafic approprié et autorisé, en refusant tout autre trafic via le pare-feu. Passez en revue les règles de pare-feu tous les six mois.

12.3 Installez un pare-feu à chaque connexion Internet et entre toute DMZ et la zone de réseau interne. Tout système stockant des informations personnelles doit résider dans la zone du réseau interne, séparé de la DMZ et des autres réseaux non fiables.

12.4 Surveillez le pare-feu au périmètre et en interne pour contrôler et protéger le flux de trafic réseau entrant ou sortant de la frontière ou de la frontière, si nécessaire.

12.5 Installez des technologies de détection des menaces telles que Network Detection and Response (NDR), Endpoint Detection and Response (EDR) et Extended Detection and Response (XDR) qui offrent une solution complète pour détecter et répondre à diverses cyberattaques ou attaques de ransomware.

12.6 Maintenir un processus documenté et des contrôles en place pour détecter et gérer les tentatives non autorisées d'accès aux Informations personnelles et aux Informations confidentielles de CWT.

12.7 Lorsque vous fournissez des services et des produits Internet à CWT, protégez les informations personnelles et les informations confidentielles par la mise en place d'un réseau DMZ. Les serveurs Web fournissant des services à CWT doivent résider dans la DMZ. Tout système ou ressource d'information stockant des informations personnelles et des informations confidentielles (telles que des serveurs d'applications et de bases de données) doit résider dans un réseau interne de confiance. Le fournisseur doit utiliser DMZ pour les services et produits Internet .

12.8 Restreindre le trafic sortant non autorisé des applications traitant, stockant ou transmettant des informations personnelles et des informations confidentielles aux adresses IP au sein de la DMZ et d'Internet.

12.9 Lors de l'utilisation de technologies de réseau sans fil basées sur les radiofréquences (RF) pour exécuter ou prendre en charge des services et des produits pour CWT, le Fournisseur doit s'assurer que toutes les informations personnelles et les informations confidentielles transmises sont protégées par l'utilisation de technologies de cryptage appropriées suffisantes pour protéger la confidentialité des informations personnelles. et Informations confidentielles ; à condition, toutefois, qu'en tout état de cause, ce cryptage n'utilise pas moins de longueurs de clé de 256 bits pour le cryptage symétrique et de 2048 bits pour le cryptage asymétrique. Analysez, identifiez et désactivez régulièrement les points d'accès sans fil non autorisés.

12.10 Sécurité cloud – Lorsque les données de CWT résident sur le cloud ou que le fournisseur utilise un environnement cloud tiers, y compris, mais sans s'y limiter, l'infrastructure en tant que service (IaaS), le logiciel en tant que service (Saas) et la plate-forme en tant que service (PaaS), le fournisseur doit mettre en œuvre ou évaluer la gestion de la posture de sécurité dans le cloud pour découvrir et corriger automatiquement les menaces, les erreurs de configuration, les abus et les violations de conformité dans les clouds publics.

13. <u>Exigences de connectivité</u>

13.1 Dans le cas où le Fournisseur a, ou doit être fourni, une connectivité aux informations personnelles et aux ressources d'informations confidentielles de CWT en conjonction avec l'Accord, alors en plus de ce qui précède, si le Fournisseur a ou reçoit une connectivité à l'environnement de CWT, le Fournisseur doit, à un le minimum:

un. Utiliser uniquement les installations et les méthodologies de connexion mutuellement convenues pour interconnecter l'environnement de CWT avec les ressources du Fournisseur.

b. NE PAS établir d'interconnexion avec l'environnement de CWT sans le consentement écrit préalable de CWT.

c. Fournir à CWT l'accès à toutes les installations applicables du Fournisseur pendant les heures normales de bureau pour la maintenance et le support de tout équipement (par exemple, un routeur) fourni par CWT dans le cadre du Contrat pour la connectivité aux ressources d'Informations personnelles et d'Informations confidentielles.

ré. Utiliser tout équipement fourni par CWT dans le cadre du Contrat pour la connectivité à l'environnement de CWT uniquement pour la fourniture des services et produits ou fonctions explicitement autorisés dans le Contrat.

e. Si la méthodologie de connectivité convenue exige que le fournisseur mette en œuvre une passerelle de sécurité, conserver les journaux de toutes les sessions utilisant cette passerelle de sécurité. Ces journaux de session doivent inclure des informations suffisamment détaillées pour identifier l'utilisateur final ou l'application, l'adresse IP d'origine, l'adresse IP de destination, les ports/protocoles de service utilisés et la durée de l'accès. Ces journaux de session doivent être conservés pendant au moins six (6) mois à compter de la création de la session.

F. Autoriser CWT à recueillir des informations relatives à l'accès, y compris l'accès du Fournisseur, à l'environnement de CWT. Ces informations peuvent être collectées, conservées et analysées par CWT afin d'identifier les risques de sécurité potentiels sans préavis. Ces informations peuvent inclure des fichiers de suivi, des statistiques, des adresses réseau et les données ou écrans réels consultés ou transférés.

g. Suspendre ou résilier immédiatement toute interconnexion avec l'environnement de CWT si les Fournisseurs pensent qu'il y a eu une violation ou un accès non autorisé ou sur les instructions de CWT si CWT, à sa seule discrétion, pense qu'il y a eu une violation de la sécurité ou un accès non autorisé ou une mauvaise utilisation des installations de données de CWT ou toute information, système ou autre ressource de CWT.

14. <u>Appareils mobiles et portables</u>

Le vendeur doit , au minimum :

14.1 Ne pas stocker d'informations personnelles et d'informations confidentielles sur des appareils mobiles et portables, à moins qu'elles ne soient entièrement cryptées à l'aide d'un cryptage fort.

14.2 Utilisez le cryptage fort pour protéger les informations personnelles et les informations confidentielles transmises, utilisées ou accessibles à distance par les appareils mobiles et portables sensibles au réseau.

un. Lors de l'utilisation d'appareils mobiles et portables compatibles avec le réseau qui ne sont pas des ordinateurs portables pour accéder et/ou stocker des informations personnelles et des informations confidentielles, ces appareils doivent être capables de supprimer toutes les copies stockées des informations personnelles et des informations confidentielles dès réception sur le réseau d'un commande. (Remarque : cette fonctionnalité est souvent appelée fonctionnalité « effacement à distance ».)

b. Avoir des politiques, des procédures et des normes documentées en place pour s'assurer que la partie autorisée qui devrait avoir le contrôle physique d'un appareil mobile et portable sensible au réseau qui n'est pas un ordinateur portable et qui stocke des informations personnelles et des informations confidentielles initie rapidement la suppression de tous Informations personnelles et informations confidentielles lorsque l'appareil est perdu ou volé.

c. Avoir des politiques, des procédures et des normes documentées en place pour garantir que les appareils mobiles et portables qui ne sont pas des ordinateurs portables et qui ne sont pas compatibles avec le réseau suppriment automatiquement toutes les copies stockées des informations personnelles et des informations confidentielles après des tentatives de connexion infructueuses consécutives.

14.3 Avoir des politiques, des procédures et des normes documentées en place qui garantissent que tous les appareils mobiles et portables utilisés pour accéder et/ou stocker des informations personnelles et des informations confidentielles :

un. Sont en la possession physique des Parties Autorisées ;
b. Sont physiquement sécurisés lorsqu'ils ne sont pas en la possession physique des Parties autorisées ; ou
c. Avoir leur stockage de données rapidement et en toute sécurité supprimé lorsqu'il n'est pas en la possession physique d' une Partie autorisée, ou physiquement sécurisé, ou après 10 tentatives d'accès infructueuses.

14.4 Avant d'autoriser l'accès aux informations personnelles et aux informations confidentielles stockées sur ou via l'utilisation d' appareils mobiles et portables, le fournisseur doit avoir et utiliser un processus pour s'assurer que :

un. L'utilisateur est une Partie Autorisée autorisée pour un tel accès ; et
b. L'identité de l'utilisateur a été authentifiée.

14.5 Mettre en œuvre une politique qui interdit l'utilisation de tout appareil mobile et portable qui n'est pas administré et/ou géré par le fournisseur ou CWT pour accéder et/ou stocker des informations personnelles et des informations confidentielles.

14.6 Examiner, au moins une fois par an, l'utilisation et les contrôles de tous les appareils mobiles et portables administrés ou gérés par le fournisseur pour s'assurer que les appareils mobiles et portables peuvent respecter les mesures de sécurité techniques et organisationnelles applicables.

15. <u>Sécurité en transit</u>

Le vendeur doit , au minimum :

15.1 Utilisez le cryptage fort pour le transfert d'informations personnelles et d'informations confidentielles en dehors des réseaux contrôlés par CWT ou contrôlés par le fournisseur ou lors de la transmission d'informations personnelles et d'informations confidentielles sur tout réseau non fiable.

15.2 Pour les enregistrements contenant des informations personnelles et des informations confidentielles au format papier, microfiche ou support électronique à transférer physiquement, transportez-les par courrier sécurisé ou par un autre mode de livraison qui peut être suivi, emballé en toute sécurité et selon les spécifications du fabricant. Toutes les

informations personnelles et les informations confidentielles doivent être transportées dans des conteneurs verrouillés.

16. <u>Sécurité au repos</u>

Le vendeur doit , au minimum :

16.1 Utilisez le cryptage fort pour protéger les informations personnelles et les informations confidentielles lorsqu'elles sont stockées.

16.2 Ne pas stocker les informations personnelles ou les informations confidentielles par voie électronique en dehors de l'environnement réseau du fournisseur (ou du propre réseau informatique sécurisé de CWT) à moins que le périphérique de stockage (par exemple, bande de sauvegarde, ordinateur portable, clé USB, disque d'ordinateur, etc.) ne soit protégé par un cryptage fort.

16.3 Ne pas stocker d'informations personnelles ou d'informations confidentielles sur des supports amovibles (par exemple, des clés USB, des clés USB, des clés USB, des bandes, des CD ou des disques durs externes), sauf : à des fins de sauvegarde, de continuité des activités, de reprise après sinistre et d'échange de données, comme autorisé et requis en vertu du contrat entre le fournisseur et CWT. Si un support amovible est utilisé pour stocker des informations personnelles ou des informations confidentielles conformément aux exceptions indiquées dans cette sous-section, les informations doivent être protégées à l'aide d'un cryptage fort. L'exécution automatique doit être désactivée pour les supports amovibles et les périphériques de stockage .

16.4 Conservez et sécurisez de manière appropriée les dossiers contenant des informations personnelles ou des informations confidentielles au format papier ou sur microfiche dans des zones dont l'accès est limité au personnel autorisé.

16.5 Sauf instruction écrite contraire de CWT, lors de la collecte, de la génération ou de la création d'informations personnelles ou d'informations confidentielles sous forme papier et sur des supports de sauvegarde pour, par l'intermédiaire ou au nom de CWT ou sous la marque CWT, assurez-vous que ces informations doivent être des informations personnelles ou des informations confidentielles. et, dans la mesure du possible, étiqueter ces informations de CWT comme « confidentielles ». Le Fournisseur reconnaît que les Informations personnelles et les Informations confidentielles sont et resteront la propriété de CWT, indépendamment de l'étiquetage ou de l'absence de celui-ci.

17. <u>Retour, conservation, destruction et élimination</u>

Le vendeur doit , au minimum :

17.1 Sans frais supplémentaires pour CWT , à la demande de CWT ou à la résiliation du Contrat , fournir des copies de toute Information personnelle et Information confidentielle à CWT dans les trente (30) jours calendaires suivant cette demande ou la résiliation du Contrat . Le

Fournisseur doit restituer ou, au choix de CWT, détruire toutes les Informations confidentielles et les Informations personnelles de CWT, y compris les copies de sauvegarde électroniques , papier et sécurisées , comme prévu dans le Contrat ou, si cela n'est pas prévu dans le Contrat, dans un délai de quatre-vingt-dix (90) jours après la plus proche des dates suivantes : (a) l'expiration ou la résiliation du Contrat, (b) la demande de retour d'Informations personnelles et d'Informations confidentielles de CWT, ou (c) la date à laquelle le Fournisseur n'a plus besoin d'Informations personnelles et d'Informations confidentielles pour fournir des services et produits visés par l'Accord.

17.2 Dans le cas où CWT approuve la destruction comme alternative au retour des Informations personnelles et des Informations confidentielles, certifier par écrit , par un agent du Vendeur, que la destruction rend les Informations personnelles et les Informations confidentielles irrécupérables et irrécupérables. Le fournisseur doit détruire complètement toutes les copies des informations personnelles et des informations confidentielles à tous les endroits et dans tous les systèmes où les informations personnelles et les informations confidentielles sont stockées, y compris, mais sans s'y limiter, les parties autorisées préalablement approuvées. Ces informations doivent être détruites en suivant une procédure standard de l'industrie pour une destruction complète telle que DOD 5220.22M ou NIST Special Publication 800-88 ou en utilisant un produit de démagnétisation recommandé par le fabricant pour le système concerné. Avant une telle destruction, le fournisseur doit maintenir toutes les mesures de sécurité techniques et organisationnelles applicables pour protéger la sécurité, la confidentialité et la confidentialité des informations personnelles et des informations confidentielles.

17.3 Éliminez les informations personnelles et les informations confidentielles de CWT de manière à garantir que les informations ne peuvent pas être reconstruites dans un format utilisable. Les papiers, diapositives, microfilms, microfiches et photographies doivent être éliminés par broyage croisé ou brûlage. Les matériaux contenant des informations personnelles et des informations confidentielles de CWT en attente de destruction doivent être stockés dans des conteneurs sécurisés et être transportés par un tiers sécurisé.

18. <u>Réponse aux incidents et notification</u>

Le vendeur doit , au minimum :

18.1 Avoir et utiliser un processus de gestion des incidents et des procédures connexes et doter ce processus et ces procédures de gestion des incidents de ressources spécialisées. Immédiatement, et en aucun cas plus de vingt-quatre (24) heures, informez CWT à iRespond@mycwt.com chaque fois qu'il y a une attaque suspectée ou confirmée, une intrusion, un accès non autorisé, une perte ou tout autre incident concernant les informations de CWT , des systèmes ou d'autres ressources.

18.2 Après avoir informé CWT, fournir à CWT des mises à jour régulières de l'état, y compris, mais sans s'y limiter, les mesures prises pour résoudre cet incident, à des intervalles ou à des moments convenus d'un commun accord pendant la durée de l'incident et dès que raisonnablement possible après la clôture de l'incident , fournir à CWT un rapport écrit

décrivant l'incident, les mesures prises par le Fournisseur lors de son intervention et les plans du Fournisseur pour les actions futures visant à empêcher qu'un incident similaire ne se produise.

18.3 Ne pas signaler ou divulguer publiquement une telle violation des informations, des systèmes ou d'autres ressources de CWT sans en informer au préalable CWT et travailler directement avec CWT pour informer les autorités régionales, nationales, étatiques ou locales concernées ou les services de surveillance du crédit, les personnes concernées par une telle violation, et tous les médias applicables, comme l'exige la loi.

18.4 Avoir un processus en place pour identifier rapidement les violations des contrôles de sécurité, y compris celles énoncées dans les présentes exigences de sécurité de l'information par le personnel du fournisseur ou des tiers. Les contrevenants identifiés feront l'objet de mesures disciplinaires appropriées sous réserve des lois applicables. Nonobstant ce qui précède, les contrevenants restent sous l'autorité du Vendeur ou de ses Tiers. CWT ne sera pas considéré comme l'employeur du Vendeur ou de son personnel Tiers .

19. <u>Gestion de la continuité des activités et reprise après sinistre</u>

Le vendeur doit , au minimum :

19.1 Élaborer , exploiter, gérer et réviser les plans de continuité des activités pour chaque site et les plans de reprise après sinistre pour chaque technologie de base afin de minimiser l'impact de CWT sur les services ou les produits du Fournisseur. Ces plans doivent inclure : des ressources nommées spécifiques aux fonctions de continuité des activités et de reprise après sinistre, des objectifs de temps de récupération établis et des objectifs de point de récupération, au moins une sauvegarde quotidienne des données et des systèmes, le stockage hors site des données et des systèmes de sauvegarde et d'enregistrement, des enregistrements des plans de protection et d'urgence proportionnés aux exigences de l'Accord, stocker ces dossiers et plans en toute sécurité hors site et s'assurer que ces plans sont à la disposition du Fournisseur au besoin.

19.2 À la demande de CWT, fournir à CWT un plan de continuité des activités documenté qui garantit que le Fournisseur peut respecter ses obligations contractuelles en vertu du Contrat et du présent document , y compris les exigences de tout énoncé de travail ou accord de niveau de service applicable. Ces plans doivent exercer la récupération tout en protégeant l'intégrité et la confidentialité des informations personnelles et des informations confidentielles.

19.3 Avoir des procédures documentées pour la sauvegarde et la récupération sécurisées des Informations personnelles et des Informations confidentielles qui doivent inclure, au minimum, des procédures pour le transport, le stockage et l'élimination des copies de sauvegarde des Informations personnelles et des Informations confidentielles et, à la demande de CWT, fournir ces procédures documentées à CWT.

19.4 Assurez-vous que des sauvegardes de toutes les informations personnelles et confidentielles stockées ou des logiciels et configurations des systèmes utilisés par CWT sont créées au moins une fois par semaine.

19.5 Les plans de continuité des activités et de reprise après sinistre doivent être mis à jour au moins une fois par an, ou aussi souvent que l'exigent des modifications importantes de l'environnement commercial et/ou technologique.

19.6 Ces plans doivent également être exercés de manière compréhensible au moins une fois par an, ou à la suite de tout changement important dans les plans de continuité des activités ou de reprise après sinistre aux frais et dépens exclusifs du Fournisseur. Ces exercices garantissent le bon fonctionnement des technologies concernées et la connaissance interne de ces plans.

19.7 Examiner rapidement son plan de continuité des activités pour traiter les sources ou scénarios de menaces supplémentaires ou émergentes et fournir à CWT un résumé de haut niveau des plans et des tests dans un délai raisonnable sur demande.

19.8 Veiller à ce que tous les sites du Fournisseur ou sous contrat avec le Fournisseur hébergeant ou traitant des Informations personnelles et des Informations confidentielles de CWT soient surveillés 24 heures sur 24, sept (7) jours sur sept contre les intrusions, les incendies, l'eau et autres risques environnementaux.

20. Conformité et accréditations

Le vendeur doit , au minimum :

20.1 Conserver des enregistrements complets et exacts relatifs à l'exécution de ses obligations découlant de ces exigences de sécurité de l'information et de la conformité du fournisseur à celles-ci dans un format permettant une évaluation ou un audit pendant une période d'au moins trois (3) ans ou plus selon les besoins en vertu d'une ordonnance d'un tribunal ou d'une procédure civile ou réglementaire. Nonobstant ce qui précède, le Fournisseur ne sera tenu de conserver les journaux de sécurité que pendant au moins un (1) an après toute exécution continue du Contrat.

20.2 Autoriser CWT, sans frais supplémentaires pour CWT, moyennant un préavis raisonnable, à effectuer des évaluations de sécurité périodiques ou des audits de la Mesure de sécurité technique et organisationnelle utilisée par le Fournisseur au cours desquels CWT fournira au Fournisseur des questionnaires écrits et des demandes de documentation. Pour toutes les demandes, le Fournisseur répondra par une réponse écrite et des preuves, le cas échéant, immédiatement ou d'un commun accord. À la demande de CWT pour un audit par CWT, le Fournisseur doit programmer un audit de sécurité devant commencer dans les dix (10) jours ouvrables suivant cette demande. CWT peut exiger l'accès aux installations, systèmes, processus ou procédures pour évaluer l'environnement de contrôle de sécurité du Fournisseur.

20.3 À la demande de CWT, certifier qu'il est en conformité avec ce document ainsi que les certifications à l'appui pour les versions les plus récentes de PCI-DSS, ISO 27001/27002, SOC

2, Cyber Essentials ou une évaluation similaire pour le Fournisseur et pour tout sous-traitant ou tiers traitement, accès, stockage ou gestion pour le compte du vendeur. Si le fournisseur n'est pas en mesure de certifier la conformité, il doit fournir un rapport écrit détaillant les points de non-conformité et son plan de remédiation pour se mettre en conformité.

20.4 Dans le cas où CWT, à sa seule discrétion, estime qu'une faille de sécurité s'est produite et n'a pas été signalée à CWT conformément au présent Contrat et au Processus de gestion des incidents du Fournisseur, programmer l'audit ou l'évaluation pour qu'il commence dans les vingt-quatre (24) heures. de l'avis de CWT exigeant une évaluation ou une vérification.

20.5 Dans les trente (30) jours calendaires suivant la réception des résultats de l'évaluation ou du rapport d'audit, fournir à CWT un rapport écrit décrivant les actions correctives que le Fournisseur a mises en œuvre ou propose de mettre en œuvre avec le calendrier et l'état actuel de chaque action corrective. Le Fournisseur mettra à jour ce rapport à CWT tous les trente (30) jours calendaires en signalant l'état de toutes les actions correctives jusqu'à la date de mise en œuvre. Le Fournisseur doit mettre en œuvre toutes les actions correctives dans les quatre-vingt-dix (90) jours suivant la réception par le Fournisseur du rapport d'évaluation ou d'audit ou dans un autre délai, à condition que ce délai alternatif ait été mutuellement convenu par écrit par les parties dans un délai maximum de trente (30) jours suivant la réception par le Fournisseur du rapport d'évaluation ou d'audit.

20.6 Conformité PCI DSS - Dans la mesure où le fournisseur gère les numéros de compte de paiement ou toute autre information de paiement connexe, le fournisseur doit être actuellement conforme à la version la plus récente de l'industrie des cartes de paiement (PCI-DSS) pour l'ensemble des systèmes traitant ces informations et continuer une telle conformité. Si un sous-traitant ou un tiers traite, accède, stocke ou gère des données de carte de crédit pour le compte du Vendeur, le vendeur doit obtenir un PCI AOC de ce sous-traitant ou tiers et le mettre à la disposition de CWT sur demande. Dans le cas où le Fournisseur n'est pas ou n'est plus conforme à la norme PCI-DSS pour toute partie de l'ensemble des systèmes traitant des données applicables à la norme PCI, le Fournisseur informera CWT dans les plus brefs délais, procédera immédiatement et sans retard injustifié pour remédier à cette non-conformité et fournira statut régulier de ces mesures correctives à CWT sur demande.

21. Normes, meilleures pratiques, réglementations et lois

Dans le cas où le Fournisseur traite, accède, visualise, stocke ou gère des informations personnelles ou des informations confidentielles concernant le personnel, les partenaires, les sociétés affiliées ou les clients de CWT ; ou les employés, sous-traitants, sous-traitants ou fournisseurs des clients de CWT ; Le fournisseur doit utiliser des mesures de sécurité techniques et organisationnelles non moins strictes que celles requises par les directives, réglementations, directives et lois applicables au niveau mondial, régional, national, étatique et local.

22. Modification

CWT se réserve le droit de mettre à jour ou de modifier ces exigences de sécurité de l'information de temps à autre en publiant la dernière version sur le site Web de CWT. À moins

que le Vendeur ne fournisse une notification écrite s'opposant à ces mises à jour ou modifications dans les trente (30) jours suivant leur publication, le Vendeur sera réputé les avoir acceptées.

Édition 6 .1
Date : avril 2024