French (European)

Exigences de Sécurité de l'Information

1. Introduction

Le Fournisseur convient que lui-même et les tierces parties agissant pour son compte en vue de fournir des services et des produits à CWT doivent se conformer aux exigences de sécurité de l'information (« **Exigences de Sécurité de l'Information** »), qui stipulent les mesures de sécurité de l'information nécessaires (« **Mesures de Sécurité Techniques et Organisationnelles** »).

2. Définitions

2.1 Sauf indication contraire stipulée dans les présentes, les termes définis ont la même signification que dans le Contrat principal. Les termes ci-dessous s'appliquent aux Exigences de Sécurité de l'Information :

« **Filiales** », sauf précision contraire dans le Contrat, désigne une partie, société ou autre entité juridique qui : (i) contrôle, soit directement, soit indirectement, une partie, ou (ii) est contrôlée, directement ou indirectement, par une partie, ou (iii) est directement ou indirectement contrôlée par une société ou une entité qui contrôle, directement ou indirectement, une partie. À ces fins, « contrôle » désigne le droit d'exercer cinquante pour cent (50%) des droits de vote ou un droit similaire de propriété, mais seulement tant que ce contrôle continue d'exister.

« Contrat », sauf précision contraire dans les modalités principales du contrat, désigne le contrat ou tout autre document juridique conclu entre CWT et le Fournisseur.

« Informations confidentielles » désigne toute information de nature commerciale sensible, exclusive ou autrement confidentielle qui a rapport (a) à CWT et ses Filiales ; (b) à un client de CWT ; (c) aux employés de CWT ; (d) aux partenaires indépendants de CWT et à ses coentreprises ou (e) au contenu et/ou à l'objet du Contrat, que ce soit à l'oral, par écrit, ou qui pourrait, par n'importe quel autre moyen, entrer directement ou indirectement en possession du Fournisseur, ou en possession d'un employé du Fournisseur, ou des représentants, des employés, des entrepreneurs ou des sous-traitants du Fournisseur, suite au Contrat ou en rapport avec celui-ci. Pour éviter toute ambiguïté, tout produit du travail constitue une Information confidentielle.

« CWT », sauf précision contraire dans le Contrat, désigne l'entité CWT à laquelle il est fait référence dans le Contrat, ainsi que ses Filiales.

« Zone démilitarisée » ou « **DMZ** » est un réseau, ou un sous-réseau, qui se trouve entre un réseau interne de confiance, tel qu'un réseau local (LAN) privé de société, et un réseau externe non sécurisé, tel que l'internet public. Une DMZ est destinée à empêcher les utilisateurs extérieurs d'avoir un accès direct aux systèmes internes et à d'autres ressources.

« Procédé de Gestion d'un Incident » désigne un procédé développé et documenté par le Fournisseur et une procédure à suivre en cas d'attaque, d'intrusion, d'accès non autorisé, de perte ou d'autre violation réelle ou supposée qui concerne la confidentialité, la disponibilité ou l'intégrité des Informations confidentielles et des Informations personnelles.

« Masquage » désigne le procédé qui consiste à cacher l'information qui apparaît à l'écran.
« Dispositifs mobiles et portables » désigne les ordinateurs, les dispositifs, les supports et systèmes mobiles et/ou portables, qui peuvent être facilement portés, déplacés, transportés ou transmis, et qui sont utilisés avec le Contrat. Ces dispositifs incluent notamment les ordinateurs portables, les tablettes, les disques durs USB, les clés USB, les PDA, les téléphones portables et tout autre dispositif

sans fil ou périphérique qui dispose de la capacité de stocker des Informations confidentielles et des Information personnelles.

« Informations personnelles » , sauf précision contraire dans le Contrat, signifie comme défini par le Règlement (UE) 2016/679 et toutes les autres lois internationales applicables concernant la sécurité des informations, la protection des données, et le respect de la vie privée, désigne toute information concernant une personne physique identifiée ou identifiable, qui peut être identifiée directement ou indirectement, notamment sur la base d'un numéro d'identification, ou d'un ou plusieurs éléments caractéristiques de son identité physique, physiologique, mentale, économique, culturelle ou sociale.

« Passerelle de sécurité » désigne un ensemble de mécanismes de contrôle entre deux ou plusieurs réseaux qui disposent de niveaux de confiance différents. Ils filtrent et enregistrent le trafic de passage ou de tentative de passage entre les réseaux, et les serveurs administratifs et de gestion associés. Les exemples de Passerelles de sécurité comprennent les pare-feu, les serveurs de gestion des pare-feu, les hop boxes, les contrôleurs de session en périphérie, les serveurs proxy, et les dispositifs de prévention d'intrusion.

« Authentification forte » désigne l'utilisation de mécanismes et de méthodologies d'authentification plus robustes que les mots de passe requis par la présente. Les exemples de mécanismes et de méthodologies d'Authentification forte comprennent les certificats numériques, l'authentification à deux facteurs et les mots de passe à usage unique.

« Cryptage fort » désigne l'utilisation de technologies de cryptage possédant des clés d'une longueur minimum de 256 bits pour le cryptage symétrique, et de 1024 bits pour le cryptage asymétrique, dont la robustesse apporte la garantie suffisante qu'il pourra protéger l'information cryptée d'un accès non autorisé et qu'il est apte à protéger la confidentialité et la nature privée de l'information cryptée, et qui applique une politique documentée de gestion des clés de cryptage et des procédés associés pour protéger la confidentialité et la nature privée des clés et des mots de passe utilisés comme éléments de saisie par l'algorithme de cryptage. Le Cryptage fort comprend, mais ne se limite pas à : SSL v3.0+/TLS v1.0+, le protocole de tunnel point à point (PPTP), AES 256, FIPS 140-2 (seulement pour le gouvernement des États-Unis), RSA 1024 bit, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4, ou WPA2.

« Mesures de sécurité techniques et organisationnelles » désigne toute activité nécessaire dans le cadre des présentes Exigences de Sécurité de l'Information pour permettre l'accès, la gestion, le transfert, le traitement, le stockage, la conservation et la destruction des informations ou données, pour révéler et informer les parties concernées, tel que prévu par le contrat et par les lois sur les informations confidentielles et la protection des données applicables, et pour protéger les informations et les données afin de garantir leur disponibilité, intégrité, confidentialité et caractère privé, ou pour informer les personnes de toute incapacité à protéger de telles informations ou données. Ces mesures comprennent mais ne se limitent pas à celles nécessaires ou jugées nécessaires en vertu des Directives de l'Union européenne 94/46/EC et 2006/24/EC telles que promulguées par les pays membres, la loi américaine Gramm-Leach Bliley (GLBA), la loi américaine sur la Portabilité et la Responsabilité de l'Assurance Médicale (HIPAA), les exigences européennes et suisses en matière de confidentialité des données, et tout autre loi internationale ou américaine, interprétation juridique officielle, ou précédent juridique relatif aux informations ou données du Contrat.

« **Tierce partie »**, sauf précision contraire dans le Contrat, désigne tout sous-traitant, et chaque intérimaire travaillant pour le Fournisseur, entrepreneur, ou fournisseur supplémentaire et/ou représentant agissant pour le compte du Fournisseur, et comprend toute définition de Tierce personne en vertu du droit européen, américain ou de tout autre droit international.

« Fournisseur » désigne l'entité adjudicatrice stipulée dans le Contrat, ainsi que ses Filiales et ses Tierces parties.

2.2 Le Fournisseur certifie qu'il respectera les Mesures de Sécurité Techniques et Organisationnelles dans la mesure où elles s'appliquent à la prestation des services stipulés dans le Contrat :

3. Organisation de la Sécurité de l'Information

Le Fournisseur devra :

3.1 Établir, mettre en œuvre et poursuivre des politiques et un programme de Mesures de Sécurité Techniques et Organisationnelles, sur les plans opérationnels, administratifs et physiques cohérents avec les pratiques du secteur mais au minimum raisonnables et appropriés afin (1) d'éviter tout accès non autorisé par le Contrat, ou par les Exigences de Sécurité de l'Information, aux Informations confidentielles et aux Informations personnelles, et (2) respecter toutes les normes du secteur qui s'appliquent. Le Fournisseur s'assurera par ailleurs que son personnel de sécurité dispose d'une expérience raisonnable et nécessaire en matière de sécurité de l'information.

3.2 Fournir un niveau approprié de supervision, de conseil et de formation sur les Mesures de Sécurité Techniques et Organisationnelles aux employés du Fournisseur qui nécessitent un accès aux Informations confidentielles et aux Informations personnelles. Le Fournisseur dispensera également une formation sur les Mesures de Sécurité Techniques et Organisationnelles à l'embauche, et avant tout accès aux Informations confidentielles et aux Informations personnelles. Des séances de remise à niveau seront mises en place au moins une fois par an, et dès que possible après qu'un changement matériel ne soit intervenu dans les Mesures de Sécurité Techniques et Organisationnelles du Fournisseur.

3.3 Les employés du Fournisseur qui ont des responsabilités de sécurité importantes, comprenant mais ne se limitant pas aux fonctions des ressources humaines ou de la technologie de l'information, et toute fonction d'administrateur de technologie, devront également recevoir une formation propre à leur poste respectif. Selon le poste, la formation spécialisée couvrira les procédures de sécurité de l'information, l'utilisation appropriée des ressources de sécurité de l'information, les risques actuels qui menacent les systèmes d'information, les fonctionnalités de sécurité de systèmes particuliers et les procédures d'accès sécurisé.

3.4 Prendre toutes les mesures raisonnables pour empêcher l'accès non autorisé aux Informations confidentielles et aux Informations personnelles et aux services, systèmes, dispositifs ou supports contenant ces informations, et éviter la perte d'Informations confidentielles ou d' Informations personnelles.

3.5 Utiliser des procédés et des procédures d'évaluation des risques pour évaluer régulièrement les systèmes utilisés dans la prestation des services ou des produits de CWT. Le Fournisseur gérera également les risques en question, et ce, dès qu'il sera raisonnablement possible de le faire, et il interviendra en fonction du niveau de risque auquel sont exposées les Informations confidentielles et les Informations personnelles, et en fonction des risques connus au moment de leur identification. Utiliser un procédé pour permettre aux employés du Fournisseur de signaler les risques ou les accidents présumés à l'équipe de sécurité du Fournisseur.

3.6 Respecter, dans la mesure où le Fournisseur délivre des services conformément au Contrat dans les installations de CWT, ou en utilisant les services, systèmes, dispositifs ou supports appartenant à CWT ou gérés par ce dernier, toutes les politiques de CWT qui ont été transmises au Fournisseur et qui

s'appliquent à un tel accès. Le Fournisseur devra par ailleurs rapidement informer CWT par écrit lorsqu'un tel accès n'est plus requis, y compris et sans exception, lorsqu'un employé, un entrepreneur, ou une tierce partie du Fournisseur ne délivrera plus de services dans le cadre du Contrat, ou lorsqu'il/elle n'aura plus accès aux Informations confidentielles et aux Informations personnelles.

3.7 Tenir un registre des ressources du Fournisseur qui transfèrent, conservent, stockent ou traitent les Informations confidentielles et aux Informations confidentielles ou y ont accès.

3.8 Satisfaire aux exigences relatives au contrôle d'antécédents de CWT dans la mesure nécessaire et autorisée par la loi, et dans les conditions prévues dans tout énoncé des travaux / bon de travaux / bon de commande qui s'applique.

4. La sécurité physique et environnementale

Le Fournisseur devra :

4.1 S'assurer que tous les systèmes et autres ressources du Fournisseur destinés à l'utilisation de plusieurs utilisateurs se trouvent dans des installations physiques sécurisées avec un accès limité et réservé aux seules personnes autorisées.

4.2 À des fins d'audit, surveiller et enregistrer l'accès aux installations physiques qui contiennent les systèmes et autres ressources destinés à l'utilisation de plusieurs utilisateurs dans le cadre des obligations de service du Fournisseur en vertu du Contrat.

4.3 S'assurer que tous les employés du Fournisseur ont signé un accord de non-divulgation ou de confidentialité avec le Fournisseur avant d'avoir accès aux Informations confidentielles et aux Informations personnelles.

4.4 Exiger de tous ses employés qu'ils respectent une politique de bureau propre et qu'ils verrouillent leur écran d'ordinateur avant de quitter leur espace de travail.

4.5 Récupérer tous les biens de la société au moment de la cessation d'emploi ou à la résiliation du contrat.

4.6 Limiter et surveiller l'accès physique à ses installations conformément aux exigences suivantes :

a. L'accès d'un visiteur est enregistré et le registre correspondant est conservé pendant trois (3) mois avec mention du nom du visiteur, de la société qu'il représente, et le nom de l'employé ayant autorisé l'accès physique.
b. L'accès est réservé aux employés compétents, en fonction de la nécessité de connaître l'accès.
c. Tous les employés doivent porter un badge fourni par la société avec leur nom.
d. En cas de résiliation, l'accès sera immédiatement retiré et tous les mécanismes permettant l'accès physique, tels que les clefs, les cartes d'accès, etc. devront être rendus ou désactivés.
e. Le centre de données ou la salle des ordinateurs est fermé à clef et l'accès en est limité aux seules personnes qui ont besoin d'y accéder pour effectuer les tâches requises par leurs fonctions.
f. Lorsque la loi l'autorise, utiliser des caméras de surveillance pour contrôler l'accès physique des individus aux zones sensibles et visionner ces données régulièrement. Les enregistrements vidéo doivent être conservés pour une durée minimum de trois (3) mois.
g. L'équipement utilisé pour stocker, traiter et transmettre les Informations confidentielles et les Informations personnelles doit être physiquement sécurisé, y compris les points d'accès sans fil,

les passerelles, les dispositifs portatifs, le matériel de réseau/communication et les lignes téléphoniques.

4.7 Mettre en place des contrôles pour limiter les risques et se protéger des menaces physiques.

4.8 Gérer l'entretien de tous les équipements traitant ou gérant des Informations confidentielles et des Informations personnelles conformément aux recommandations d'entretien applicables aux tierces parties prestataires de services.

4.9 Limiter l'accès aux prises de réseaux des salles de conférence ou d'autres réseaux du Fournisseur qui sont accessibles au public et dont l'accès est limité aux seuls utilisateurs authentifiés, ou désactivés par défaut.

4.10 Protéger tout dispositif de capture de données de carte de paiement par une interaction physique directe contre un sabotage et une substitution en inspectant régulièrement l'extérieur du dispositif pour déceler un sabotage ou une substitution éventuel, et dispensera une formation à ses employés pour les sensibiliser aux tentatives de sabotage ou de remplacement des dispositifs.

4.11 Contrôler et dissocier les points d'accès tels que les zones de livraison et de chargement et les autres points dans tous les centres gérant, stockant et traitant des Informations confidentielles et des Informations personnelles, ou ayant accès à celles-ci.

4.12 Équiper impérativement les centres de données de dispositifs de chauffage, de refroidissement, de protection incendie, de détection d'eau et de détection de chaleur/fumée.

5. Contrôle d'accès

Le Fournisseur devra:

5.1 Prendre toutes les mesures raisonnables pour empêcher toute personne d'accéder aux Informations confidentielles et aux Informations personnelles de quelque manière ou pour tout objectif que ce soit non autorisé par CWT et par le Contrat. Le Fournisseur limitera également l'accès aux Informations confidentielles et aux Informations personnelles aux employés du Fournisseur qui (1) ont un besoin légitime d'accéder aux Informations confidentielles et aux Informations personnelles pour la prestation de services conformément au Contrat, et (2) ont donné leur accord écrit pour protéger l'intégrité, la disponibilité et la confidentialité des Informations confidentielles et des Informations personnelles.

5.2 Mettre en place des procédures raisonnables pour mettre un terme à l'accès aux informations confidentielles et aux Informations personnelles fourni aux employés du Fournisseur lorsque cela n'est plus nécessaire, ni requis pour leur travail, et avant la fin de leur contrat avec le Fournisseur ou de leur mission auprès de CWT.

5.3 Séparer les informations de CWT des applications et informations d'autres clients ou de celles qui sont propres au 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 implémentée.

5.4 Identifier et demander aux propriétaires légitimes de vérifier et d'approuver l'accès aux systèmes utilisés pour traiter, gérer, stocker les Informations confidentielles et les Informations personnelles ou y accéder, et maintenir et réaliser un suivi des autorisations d'accès.

5.5 Annuler l'accès aux systèmes qui gèrent les Informations confidentielles et les Informations personnelles dans les 24 heures qui suivent la cessation de relation entre un employé, un entrepreneur, un sous-traitant ou une tierce partie et le Fournisseur, et annuler l'accès à ces systèmes dans les trois (3) jours ouvrables qui suivent le changement de responsabilité d'un employé, entrepreneur, sous-traitant, ou tierce personne dans la société. Tous les autres identifiants d'utilisateurs doivent être désactivés ou éliminés après 90 jours civils d'inactivité.

5.6 Vérifier et approuver régulièrement l'accès aux systèmes qui gèrent les Informations personnelles aux Informations confidentielles et aux Informations personnelles au moins une fois tous les trimestres pour éliminer les accès non autorisés.

5.7 Restreindre l'accès de l'administrateur du système (également connu sous le nom d'accès root, d'utilisateur privilégié ou de super utilisateur) aux systèmes d'exploitation destinés à l'utilisation de plusieurs utilisateurs aux seules personnes qui nécessitent un tel niveau élevé d'accès pour effectuer leur travail. Dans la mesure du possible, utiliser des identifiants de « check out » avec des identifiants de connexion et des journaux d'activité d'utilisateur individuel pour gérer l'accès hautement sécurisé, et dans le cas contraire, réduire l'accès de niveau élevé à un nombre très limité d'utilisateurs.

5.8 Exiger que l'application, la base de données, le réseau et les administrateurs du système restreignent l'accès des utilisateurs aux seuls commandes, données, systèmes et autres ressources nécessaires à l'accomplissement des fonctions qui leur sont autorisées.

5.9 Exiger une Authentification forte pour tout accès à distance.

5.10 Interdire et utiliser des Mesures de Sécurité Techniques et Organisationnelles pour s'assurer que les employés du Fournisseur qui accèdent aux Informations confidentielles et aux Informations personnelles ne puissent pas copier, déplacer ou stocker d'Informations confidentielles ou d'Informations personnelles sur des disques durs locaux, ni couper/coller ou imprimer d'Informations confidentielles ou d'Informations personnelles.

5.11 Activer l'utilisation des capacités d'accès à distance uniquement en cas de nécessité, surveiller durant l'utilisation et désactiver immédiatement après utilisation.

5.12 Exiger au moins une authentification à deux facteurs pour se connecter aux ressources internes du Fournisseur qui contiennent des Informations confidentielles et des Informations personnelles.

6. Identification etc authentification

Le Fournisseur devra :

6.1 Attribuer un identifiant d'utilisateur unique aux utilisateurs individuels et attribuer des mécanismes d'authentification à chaque compte individuel.

6.2 Utiliser un procédé documenté de gestion du cycle de vie d'un identifiant d'utilisateur pour tout accès aux Informations confidentielles et aux Informations personnelles, et pour tous les environnements (par ex. de production, de test, de développement, etc.), mais sans se limiter aux procédures de création de comptes approuvés, de suppression de compte en temps opportun, et de modification de compte (par ex. une modification des privilèges, de niveaux d'accès, de fonctions/postes). Un tel procédé inclura une vérification des privilèges d'accès et de la validité du compte et aura lieu au moins tous les trimestres.

6.3 Appliquer la règle du moindre privilège (c.-à-d. limiter l'accès aux seuls commandes, informations, systèmes et autres ressources nécessaires à accomplir les fonctions autorisées selon le poste de la personne).

6.4 Restreindre tout accès aux Informations confidentielles et aux Informations personnelles nécessitant un identifiant d'utilisateur et un mot de passe valides et exiger un identifiant d'utilisateur unique pour utiliser l'un des éléments suivants : mot de passe ou phrase-code, authentification à deux facteurs ou valeur biométrique.

6.5 Exiger un mot de passe complexe qui réponde aux exigences de création de mot de passe suivantes : une longueur minimum de huit (8) caractères pour les mots de passe du système et de quatre (4) caractères pour les mots de passe de tablettes et de smartphones. Les mots de passe du système doivent contenir trois (3) des éléments suivants : une lettre majuscule, une lettre minuscule, un caractère numérique ou spécial. Les mots de passe ne doivent pas non plus être les mêmes que les identifiants d'utilisateur auxquels ils sont associés, ne doivent pas contenir de mot du dictionnaire, de nombres séquentiels ou répétés, et ne doivent pas être l'un des cinq derniers mots de passe. Exiger qu'une expiration du mot de passe à intervalles réguliers n'excède pas quatre-vingt-dix (90) jours. Masquer tous les mots de passe lorsqu'ils apparaissent à l'écran.

6.6 Limiter les tentatives de connexion pour qu'elles ne dépassent pas cinq (5) tentatives infructueuses de connexion dans les 24h et verrouiller le compte d'utilisateur de façon permanente une fois cette limite atteinte. L'accès au compte d'utilisateur peut être réactivé par la suite grâce à un procédé manuel qui requiert la vérification de l'identité de l'utilisateur.

6.7 Vérifier l'identité de l'utilisateur et définir une utilisation unique, et réinitialiser les mots de passe pour qu'une valeur unique s'applique à chaque utilisateur. Demander une modification de façon systématique après la première utilisation.

6.8 Employer une méthode sécurisée pour communiquer les identifiants d'authentification (par ex. les mots de passe) et les mécanismes d'authentification (par ex. les jetons d'authentification ou les cartes smart).

6.9 Limiter les mots de passe du compte de service et du proxy à un minimum de 12 caractères, y compris les majuscules, les minuscules et les caractères numériques, ainsi que les symboles spéciaux. Changer les mots de passe du compte de service et du proxy au moins une fois par an.

6.10 Mettre un terme aux sessions interactives ou activer un écran de veille de verrouillage sécurisé demandant une authentification après une période d'inactivité qui ne dépasse pas quinze (15) minutes.

6.11 Utiliser une méthode d'authentification en fonction du caractère sensible des Informations confidentielles et des Informations personnelles. Une fois les identifiants d'authentification stockés, les protéger en utilisant un Cryptage fort.

6.12 Configurer les systèmes pour que la session expire après une période maximale d'inactivité : serveur (15 minutes), poste de travail (15 minutes), dispositif portable (4 heures), protocole d'attribution dynamique des adresses ou DHCP (7 jours), réseau VPN (24 heures).

7. Acquisition, développement et entretien des Systèmes d'Information

Le Fournisseur devra :

7.1 Afficher une bannière d'avertissement sur les écrans ou une page ect de connexion selon les spécifications écrites de CWT pour les produits ou services portant la marque CWT ou pour les produits ou logiciels développés pour CWT.

7.2 S'assurer que tous les employés susceptibles d'exécuter des travaux dans le cadre du Contrat respectent les Mesures de Sécurité Techniques et Opérationnelles, comme en attestera un accord écrit qui n'est pas moins limitatif que les présentes Exigences de Sécurité de l'Information.

7.3 Restituer tous les dispositifs appartenant à CWT ou fourni par ce dernier dès que possible, mais au plus tard (15) jours après que l'un des événements suivants se soit produit :

(a) expiration ou résiliation du Contrat
(b) demande de restitution d'une telle propriété par CWT, ou
(c) date à partir de laquelle le Fournisseur n'a plus besoin de tels dispositifs.

7.4 Utiliser une méthodologie de gestion d'application efficace qui incorpore les mesures techniques et organisationnelles de sécurité dans le processus de développement du logiciel, et s'assurer que lesdites mesures, telles que représentées dans le cycle de vie du développement du logiciel de CWT ou dans les politiques, les normes et les procédures de sécurité de l'information, sont appliquées en temps et en heure par le Fournisseur.

7.5 Suivre des procédures de développement standards, y compris la séparation de l'accès et du code entre les environnements de production et de non-production, et la séparation des tâches correspondantes entre lesdits environnements.

7.6 S'assurer que les contrôles internes de sécurité de l'information pour le développement de logiciel sont évalués régulièrement et qu'ils reflètent les meilleures pratiques de l'industrie. Passer en revue et implémenter ces contrôles en temps utile.

7.7 Gérer la sécurité du processus de développement et s'assurer que les pratiques sécurisées de codage sont implémentées et respectées, y compris les contrôles cryptographiques appropriés, les protections contre les codes malveillants, ainsi qu'un processus d'évaluation collégiale.

7.8 Réaliser des tests d'intrusion sur les applications fonctionnellement complètes avant leur mise en production et par la suite, au moins une fois par an, et après toute modification significative du code source ou d'une configuration en conformité avec OWASP, CERT, SANS Top 25, et PCI-DSS. Remédier à toute vulnérabilité susceptible d'être exploitée avant le déploiement en environnement de production.

7.9 Utiliser des données rendues anonymes ou obscurcies dans des environnements de non-production. Ne jamais utiliser de données de production en texte clair dans un environnement de non-production et ne jamais utiliser d'Informations personnelles ni d'Informations personnelles dans des environnements de non-production sous quelque prétexte que ce soit. S'assurer que toutes les données et comptes de test ont été effacés avant de lancer la production.

7.10 S'assurer que le Fournisseur utilisant des codes, logiciels, applications ou services open source fait preuve de diligence raisonnable en vérifiant lesdits codes obtenus pour éviter les failles, les bogues ou les problèmes de sécurité qui pourraient avoir une incidence sur l'intégrité des données, leur disponibilité ou la confidentialité de CWT ou de ses clients. Le Fournisseur devra par ailleurs avertir CWT des situations où il fait appel à du code open source, et fournir à CWT le nom et la version du code open source.

7.11 S'assurer que le Fournisseur ne partage pas les codes créés dans le cadre du Contrat, dans des environnements partagés ou non privés, tels qu'un répertoire de codes d'accès en libre accès, quelle que soit la protection du mot de passe et quel que soit le stade de développement.

8. Logiciels et intégrité des données

Le Fournisseur devra :

8.1 Lorsque des logiciels antivirus sont commercialisés pour les environnements en question, faire installer des logiciels antivirus et analyser, éliminer ou mettre en quarantaine les virus ou autres programmes malveillants pour les purger de tout système ou dispositif.

8.2 Séparer les informations et ressources de non-production des informations et ressources de production.

8.3 S'assurer que les équipes utilisent un processus documenté de contrôle des modifications pour tous les changements apportés aux systèmes, y compris des procédures de sortie pour tous les environnements de production et des processus de changement d'urgence. Inclure les tests, la documentation et les approbations pour tous les changements de systèmes et exiger l'autorisation de la direction pour tout changement significatif desdits processus.

8.4 Créer et maintenir une zone PCI si le Fournisseur traite ou stocke les données des titulaires de carte.

8.5 Pour les applications utilisant une base de données qui permet d'apporter des modifications aux Informations confidentielles et aux Informations personnelles, activer, et garder activées, les fonctionnalités de journalisation des audits de transactions dans la base de données et conserver les journaux d'audit des transactions dans la base de données pour une durée minimale de six (6) mois.

8.6 Examiner les logiciels pour identifier et corriger leurs vulnérabilités en matière de sécurité pendant la période d'implémentation initiale et après toute modification ou mise à jour significative.

8.7 Réaliser des tests de contrôle qualité pour les composants de sécurité (par ex. tests des fonctions d'identification, d'authentification et d'autorisation), et effectuer toute autre activité ayant pour objectif de valider l'architecture de sécurité, pendant la période d'implémentation initiale et après toute modification ou mise à jour significative.

9. Sécurité du système

Le Fournisseur devra :

9.1 Créer et mettre régulièrement à jour les versions les plus récentes des schémas du système et des flux de données qui sont utilisés pour traiter, gérer ou stocker les Informations confidentielles et les Informations personnelles ou y accéder.

9.2 Consulter activement les ressources du secteur (par ex. , }www.cert.org et les listes de distribution et sites internet des fournisseurs de logiciels pertinents) pour se tenir informé des alertes de sécurité qui s'appliquent et qui concernent les systèmes et autres sources d'informations du Fournisseur.

9.3 Gérer efficacement les clés cryptographiques en limitant l'accès à ces clés au nombre le plus faible possible et strictement nécessaire de dépositaires, en stockant les clés cryptographiques secrètes et privées au moyen d'une clé de chiffrement au moins aussi robuste que la clé de cryptage des données,

et en les stockant séparément de la clé de cryptage des données à l'aide d'un dispositif cryptographique sécurisé, dans un nombre d'emplacements le plus limité possible. Changer les clés cryptographiques par défaut fournies à l'installation, et au moins tous les deux ans, et se débarrasser des anciennes clés en toute sécurité.

9.4 Analyser les systèmes externes et autres sources d'information, y compris, mais sans s'y limiter, les réseaux, serveurs et applications, en utilisant des logiciels conformes aux normes applicables dans le secteur en matière de vulnérabilité et de sécurité afin de détecter les vulnérabilités de sécurité au moins tous les trimestres, et avant de valider les applications et les changements significatifs, et toute amélioration, dans les délais dépendants des analyses de risques en se basant sur les politiques et les normes de TI raisonnables et généralement acceptées.

9.5 Analyser les systèmes internes et autres sources d'information, y compris, mais sans s'y limiter, les réseaux, serveurs, applications et bases de données, en utilisant des logiciels conformes aux normes applicables dans le secteur en matière de vulnérabilité et de sécurité afin de détecter les vulnérabilités de sécurité pour s'assurer que lesdits systèmes et autres ressources sont convenablement renforcés, et identifier tout réseau sans fil non autorisé au moins tous les trimestres, et avant de valider les applications et les changements significatifs et toute amélioration dans les délais dépendants des analyses de risques en se basant sur les politiques et les normes de TI raisonnables et généralement acceptées,.

9.6 Maintenir un processus de classification des risques pour les résultats d'évaluation de vulnérabilité en se basant sur les meilleures pratiques du secteur et l'impact potentiel. Tout résultat d'évaluation obtenant un score CVSS supérieur ou égal à 4 doit être traité en appliquant une méthode validée en vue de garantir la gestion de l'évaluation permanente des risques.

9.7 S'assurer que tous les systèmes et autres ressources du Fournisseur sont et demeurent « renforcés », y compris, mais sans s'y limiter, en supprimant ou en désactivant les réseaux ou autres services ou produits non utilisés (par ex. finger, rlogin, ftp et les services et produits de protocole de contrôle de transmission/protocole internet (TCP/IP) simples), et en installant un pare-feu de système, des enveloppeurs TCP ou une technologie similaire.

9.8 Déployer un ou plusieurs systèmes de détection d'intrusion (IDS), de prévention d'intrusion (IPS) ou systèmes de détection et de prévention d'intrusion (IDP) en mode d'opération actif pour surveiller le trafic entrant et sortant des systèmes et d'autres ressources en rapport avec le Contrat lorsqu'une telle technologie est commercialisée pour ces environnements, et dans la mesure du possible.

9.9 Maintenir un processus de classement des risques pour remédier aux vulnérabilités de sécurité de tout système ou autre ressource, y compris, mais sans s'y limiter, celles identifiées grâce aux publications du secteur, à un scan de vulnérabilité, à un scan antivirus et à l'examen des journaux de sécurité, et installer les correctifs de sécurité appropriés dans les meilleurs délais, étant donné la probabilité qu'une telle vulnérabilité soit potentiellement exploitée ou en cours d'exploitation. Les correctifs critiques avec un score CVSS de 7,5 ou plus doivent être installés immédiatement dès qu'ils sont disponibles et au plus tard un mois après leur publication. Les correctifs critiques avec un score CVSS de 4 ou plus doivent être installés dans les 90 jours suivant leur publication.

9.10 Effectuer des tests d'intrusion généralisée en interne et en externe au moins une fois par an, et après chaque amélioration ou modification significative d'infrastructure ou d'application.

9.11 Supprimer ou désactiver les logiciels non autorisés qui sont découverts dans les systèmes du Fournisseur et effectuer des contrôles conformes aux standards du secteur pour détecter des programmes malveillants, y compris, l'installation, la mise à jour régulière et l'utilisation routinière de

produits logiciels contre les programmes malveillants pour tous les services, systèmes et dispositifs qui pourraient être utilisés pour accéder aux Informations confidentielles et aux Informations confidentielles. Dans la mesure du possible, utiliser des logiciels antivirus fiables et issus des meilleures pratiques du secteur et s'assurer que lesdites définitions de virus sont maintenues à jour.

9.12 S'assurer que les logiciels sont actualisés pour tous les services, systèmes et dispositifs qui pourraient être utilisés pour accéder aux Informations confidentielles et aux Informations personnelles , y compris l'entretien approprié du/des système(s) opérationnel(s) et l'installation réussie des correctifs de sécurité raisonnablement actualisés.

9.13 Assigner les responsabilités administratives liées à la sécurité qui consistent à configurer les systèmes d'exploitation hôtes à des personnes spécifiques.

9.14 Modifier tous les noms de compte et/ou mots de passe par défaut.

10. Surveillance

Le Fournisseur devra :

10.1 Conserver les journaux de données relatifs aux Informations confidentielles et aux Informations personnelles pendant au moins 12 mois et s'assurer que ces données sont mises à la disposition de CWT dans un délai raisonnable et à sa demande, sauf dispositions spécifiques dans une autre partie du Contrat.

10.2 Enregistrer les activités du système principal pour les systèmes contenant des Informations confidentielles et des Informations personnelles.

10.3 Limiter l'accès aux journaux de sécurité aux personnes autorisées, et protéger les journaux de sécurité de toute modification non autorisée.

10.4 Mettre en place un mécanisme de détection des changements (par ex. la surveillance de l'intégrité des fichiers) pour alerter les employés en cas de modification non autorisée de fichiers du système, de fichiers de configuration ou de fichiers de contenu sensibles, et configurer les logiciels pour qu'ils effectuent des comparaisons de fichiers sensibles de façon hebdomadaire.

10.5 Examiner les journaux d'audit de sécurité ou ayant trait à la sécurité issus des systèmes contenant des Informations confidentielles et des Informations personnelles afin de déceler des anomalies, et ce, au moins une fois par semaine, et documenter et résoudre dans les meilleurs délais tous les problèmes de sécurité enregistrés.

10.6 Vérifier tous les évènements ayant trait à la sécurité, les journaux de stockage des composants du système, de traitement et de transmission de données des titulaires de carte, les journaux de composants sensibles du système, et les journaux des serveurs et des composants du système qui remplissent des fonctions de sécurité, et ce, quotidiennement.

11. Passerelles de sécurité

Le Fournisseur devra :

11.1 Exiger une Authentification forte pour permettre un accès administratif et/ou de gestion aux Passerelles de sécurité, y compris, mais sans s'y limiter, tout accès ayant pour objectif d'examiner les fichiers des journaux.

11.2 Posséder et utiliser des contrôles, politiques, procédés et procédures documentés pour s'assurer que des utilisateurs non autorisés n'ont pas un 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 S'assurer, au moins une fois tous les six (6) mois, que les configurations des Passerelles de sécurité sont renforcées en sélectionnant un échantillon de Passerelles de sécurité et en vérifiant que chaque ensemble de règles et de paramètres de configuration par défaut garantit les points suivants :

a. Le mécanisme de routage source du Protocole Internet (IP) est désactivé
b. L'adresse de bouclage est soumise à une interdiction d'accès au réseau interne
c. Les filtres anti-usurpation sont en place
d. Les paquets de diffusion ne sont pas autorisés à pénétrer sur le réseau
e. La redirection du protocole de message de contrôle sur Internet (ICMP) est désactivée
f. Tous les ensembles de règles se terminent par le message "Interdire toutes tentatives", et
g. Il est possible de retrouver la requête spécifique à l'origine de chaque règle.

11.4 S'assurer que les outils de surveillance sont utilisés pour vérifier que tous les aspects concernant les Passerelles de sécurité (par ex. le matériel, les micrologiciels et logiciels) sont constamment opérationnels.

11.5 S'assurer que toutes les Passerelles de sécurité sont configurées et mises en place de façon à ce que les Passerelles de sécurité non opérationnelles refusent tout accès.

11.6 S'assurer que les paquets entrants du réseau externe non approuvé aboutissent bien dans la zone démilitarisée (« **DMZ** ») et ne soient pas autorisés à passer directement par le réseau interne approuvé. Tous les paquets entrants qui arrivent dans le réseau interne approuvé doivent provenir exclusivement de la DMZ. La DMZ doit être distincte du réseau externe non approuvé par le biais d'une Passerelle de sécurité et doit être distincte du réseau interne approuvé par le biais :

a. d'une autre Passerelle de sécurité, ou
b. de la même Passerelle de sécurité que celle utilisée pour séparer la DMZ du réseau externe non approuvé, auquel cas la Passerelle de sécurité doit garantir que les paquets reçus du réseau externe non approuvé sont soit immédiatement supprimés, soit si ce n'est pas le cas, dirigés exclusivement vers la DMZ sans recevoir d'autre traitement excepté l'écriture éventuelle de ces paquets dans un journal.

Ce qui suit doit uniquement se trouver au sein du réseau interne approuvé :

a. Toute Information confidentielle ou Information personnelle stockée sans utiliser de Cryptage fort,
b. L'enregistrement officiel des informations auxquelles l'accès est prévu à partir de requêtes provenant du réseau externe non approuvé,
c. L'enregistrement officiel des informations dont la modification est prévue suite à des requêtes provenant du réseau externe non approuvé,
d. Les serveurs de bases de données,
e. Tous les journaux exportés, et
f. Tous les environnements utilisés pour le développement, les tests, les bacs à sable, la production, et tout autre environnement semblable, ainsi que toutes les versions de code source.

11.7 Les identifiants d'authentification non protégés par l'application d'un Cryptage fort doivent se trouver dans la DMZ.

12. Sécurité du réseau

Le Fournisseur devra :

12.1 A la demande de CWT, fournir à CWT un schéma logique du réseau qui documente les systèmes et connexions aux autres ressources telles que les routeurs, les plateformes, les pare-feu, les systèmes IDS, la topologie du réseau, les points de connexion externes, les passerelles, les réseaux sans fil et tout autre dispositif qui puisse aider CWT.

12.2 Avoir en place un processus officiel pour l'approbation, les tests et la documentation de toutes les connexions sur le réseau et des changements apportés aux configurations des pare-feu et des routeurs. Configurer les pare-feu de sorte qu'ils refusent et enregistrent les paquets suspects et imposer des restrictions pour permettre uniquement le trafic approprié et autorisé, en bloquant ainsi tout autre trafic au niveau du pare-feu. Vérifier l'ensemble des règles de pare-feu tous les six mois.

12.3 Installer un pare-feu à chaque connexion internet, et entre toute DMZ et la zone de réseau interne. Tout système stockant des Informations confidentielles et des Informations personnelles doit résider dans la zone de réseau interne et être séparé de la DMZ et d'autres réseaux non sécurisés.

12.4 Surveiller le pare-feu dans le périmètre et en interne afin de contrôler et protéger le flux du trafic réseau entrant ou quittant le périmètre ou la limite, selon le besoin.

12.5 Garder en place un processus et des contrôles documentés pour détecter et gérer les tentatives d'accès non autorisées aux Informations confidentielles et aux Informations personnelles.

12.6 Dans le cas d'une prestation de services et d'une livraison de produits à CWT par l'intermédiaire d'internet, protéger les Informations confidentielles et les Informations personnelles en mettant en place un réseau DMZ. Les serveurs web qui fournissent un service à CWT devront résider dans la DMZ. Tout système ou ressource d'information stockant des Informations confidentielles et des Informations personnelles (tels que les serveurs d'application et de base données) devront résider sur un réseau interne de confiance. (Les services et produits sur internet Doivent Utiliser une DMZ).

12.7 Limiter le trafic sortant non autorisé en provenance d'applications traitant, stockant ou transmettant des Informations confidentielles et des Informations personnelles à des adresses IP dans la DMZ et sur Internet.

12.8 Dans le cas où des technologies de réseau sans fil utilisant les fréquences radio (RF) seraient utilisées pour offrir des services et des produits ou de l'assistance à CWT, s'assurer que toutes les Informations confidentielles et les Informations personnelles qui sont transmises sont protégées par l'utilisation de technologies de cryptage fort et suffisantes pour protéger la confidentialité des Informations confidentielles et des Informations personnelles. Analyser, identifier et désactiver les points d'accès sans fil non autorisés de façon régulière.

13. Exigences en matière de connectivité

Le Fournisseur devra :

13.1 Dans l'éventualité où le Fournisseur aurait, ou obtiendrait, une connectivité aux ressources d'Informations confidentielles et d' Informations personnelles dans le cadre du Contrat, alors :

a. Utiliser uniquement les installations et les méthodologies de connexion qui ont été convenues d'un commun accord pour interconnecter les ressources d'Informations confidentielles et d'Informations personnelles avec les ressources du Fournisseur.
b. Ne pas mettre en place d'interconnexion avec les ressources d'Informations confidentielles et d' Informations personnelles de CWT sans l'accord préalable de CWT.
c. Permettre l'accès de CWT à toute installation du Fournisseur qui s'applique, et ce, pendant les heures normales de travail, pour l'entretien et l'assistance technique de tout équipement (par ex. un routeur) fourni par CWT pour permettre la connectivité aux ressources d'Informations confidentielles et d'Informations personnelles de CWT dans le cadre du Contrat.
d. Utiliser l'équipement fourni par CWT pour permettre la connectivité aux ressources d'Informations confidentielles et d'Informations personnelles dans le cadre du Contrat seulement pour la prestation de services et de produits, ou fonctions explicitement autorisés par le Contrat.
e. Si la méthodologie de connectivité convenue exige que le Fournisseur mette en place une Passerelle de sécurité, maintenir des journaux pour toutes les sessions qui utilisent ladite Passerelle de sécurité. Ces journaux de session doivent contenir des informations suffisamment détaillées pour permettre d'identifier l'utilisateur final, 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 pour un minimum de six (6) mois à partir de la création de session.

13.2 Dans l'éventualité où le Fournisseur aurait, ou obtiendrait, une connectivité aux ressources d'Informations confidentielles et d'Informations personnelles dans le cadre du Contrat, en plus d'autres droits stipulés par la présente, il autorisera CWT à :

a. Rassembler des informations au sujet de l'accès, y compris de l'accès du Fournisseur, aux ressources d'Informations confidentielles et d'Informations personnelles. Ces informations pourront être recueillies, conservées et analysées par CWT afin d'identifier des risques potentiels de sécurité, et ce sans préavis. Elles peuvent comprendre des fichiers de trace, des statistiques, des adresses de réseau, ainsi que les données ou les écrans qui ont été accédés ou transférés.
b. Immédiatement interrompre ou mettre un terme à toute interconnexion aux ressources d'Informations confidentielles et d'Informations personnelles si CWT pense qu'il y a eu une atteinte à la sécurité ou un accès non autorisé, ou une utilisation frauduleuse des installations de données de CWT ou de tout système, information ou autres ressources de CWT.

14. Dispositifs mobiles et portables

Le Fournisseur devra :

14.1 Utiliser un Cryptage port afin de protéger toutes les Informations confidentielles et les Informations personnelles qui sont stockées sur des dispositifs mobiles et portables.

14.2 Ne pas stocker d'Informations confidentielles ou d'Informations personnelles sur des dispositifs mobiles ou des ordinateurs portables et ne pas stocker d'Informations confidentielles ou d'Informations personnelles sur des périphériques amovibles à moins d'utiliser un Cryptage fort.

14.3 Utiliser un Cryptage fort afin de protéger les Informations confidentielles et les Informations personnelles qui sont transmises, ou auxquelles il est possible d'accéder à distance par l'intermédiaire de dispositifs mobiles et portables utilisant le réseau.

a. Dans le cas d'une utilisation sur le réseau de dispositifs mobiles et portables, qui ne sont pas des ordinateurs portables, pour accéder et/ou stocker des Informations confidentielles ou des Informations personnelles, les dispositifs en question doivent être capables de supprimer toutes les copies d'Informations confidentielles ou d'Informations personnelles après avoir reçu une commande correctement authentifiée sur le réseau. (Remarque : Une telle capacité est souvent appelée « effacement à distance ».)
b. Mettre en place des politiques, procédures et normes documentées pour s'assurer que la personne habilitée à contrôler physiquement un dispositif mobile et portable qui n'est pas un ordinateur portable et qui stocke des Informations confidentielles ou des Informations personnelles, supprime rapidement toutes les Informations confidentielles et les Informations personnelles en cas de perte ou de vol du dispositif.
c. Mettre en place des politiques, procédures et normes documentées pour s'assurer que les dispositifs mobiles et portables qui ne sont pas des ordinateurs portables et qui ne sont pas sur le réseau, suppriment automatiquement toutes les copies d'Informations confidentielles et d'Informations personnelles après plusieurs tentatives de connexion consécutives infructueuses.

14.4 Mettre en place des politiques, procédures et normes documentées qui garantissent que tout dispositif mobile et portable utilisé pour accéder et/ou stocker des Informations confidentielles et des Informations personnelles :

a. Est physiquement détenu par la/les personne(s) autorisée(s)
b. Est en lieu sûr lorsque la personne autorisée n'est pas physiquement en sa possession, ou
c. Voit ses données stockées rapidement supprimées, et ce d'une manière sécurisée, lorsque la personne autorisée n'est pas physiquement en sa possession, ou qu'il ne se trouve pas en lieu sûr, ou après 10 tentatives d'accès infructueuses.

14.5 Avant d'autoriser l'accès aux Informations confidentielles et aux Informations personnelles qui sont stockées sur ou par l'intermédiaire de dispositifs mobiles et portables, mettre en place et utiliser un processus pour s'assurer que :

a. L'utilisateur est autorisé à avoir l'accès en question, et
b. L'identité de l'utilisateur a été authentifiée.

14.6 Mettre en place une politique interdisant l'utilisation de tout dispositif mobile et portable qui n'est pas administré et/ou géré par le Fournisseur ou CWT pour accéder à des Informations confidentielles et des Informations personnelles et/ou les stocker.

14.7 Vérifier au moins une fois par an, l'utilisation et les contrôles de tous les dispositifs mobiles et portables administrés ou gérés par le Fournisseur pour s'assurer que les dispositifs mobiles et portables puissent respecter les Mesures Techniques et Organisationnelles de Sécurité applicables.

15. Sécurité en transit

Le Fournisseur devra :

15.1 Utiliser un Cryptage fort pour transférer les Informations confidentielles et les Informations personnelles en dehors des réseaux contrôlés par CWT ou le Fournisseur ou lorsqu'il transmet les Informations confidentielles et les Informations personnelles sur des réseaux non sécurisés.

15.2 Pour les dossiers contenant des Informations confidentielles ou des Informations personnelles en version papier, sur des microfiches ou sur des supports électroniques à transférer physiquement, les transporter de façon sécurisée par un service de messagerie ou une autre méthode de livraison qui

puisse être suivie. Ils doivent être correctement emballés selon les spécifications du fabricant. Toutes les Informations confidentielles et les Informations personnelles doivent être transportées dans des contenants verrouillés.

16. Sécurité en immobilisation

Le Fournisseur devra :

16.1 Utiliser un Cryptage fort afin de protéger les Informations confidentielles et les Informations personnelles lorsque celles-ci sont stockées.

16.2 Ne pas stocker les Informations confidentielles et les Informations personnelles sous forme électronique en dehors de l'environnement de réseau du Fournisseur (ou du réseau informatique sécurisé de CWT) à moins d'avoir protégé le dispositif de stockage (par ex. bande de sauvegarde, ordinateur portable, clé USB, disque dur d'ordinateur, etc.) au moyen d'un Cryptage fort.

16.3 Ne pas stocker les Informations confidentielles et les Informations personnelles sur des supports amovibles (par ex. clés USB, cartes mémoire, bandes, CD ou disques durs externes) hormis à des fins de : (a) sauvegarde, poursuite d'activité, reprise d'activité après un sinistre et échange de données dans les limites requises et autorisées par le contrat, et (b) au moyen d'un Cryptage fort.

16.4 Convenablement stocker et sécuriser les enregistrements qui contiennent des Informations confidentielles et des Informations personnelles en version papier ou sur microfiches dans des zones dont l'accès est réservé aux personnes autorisées.

16.5 Sauf instruction contraire écrite de CWT, s'assurer, lorsqu'il rassemble, génère ou créer des Informations confidentielles et des Informations personnelles en version papier et sur un support de sauvegarde par l'intermédiaire, pour le compte ou sous la marque de CWT, que ces informations sont des Informations confidentielles et des Informations personnelles et, dans la mesure du possible, identifier ces Informations de CWT comme étant « confidentielles ». Le Fournisseur accepte que les Informations confidentielles et les Informations personnelles restent la propriété de CWT quel que soit l'étiquetage, ou même en l'absence d'étiquetage.

17. Retour, destruction et élimination

Le Fournisseur devra :

17.1 Suite à la demande de CWT, fournir les copies de toute Information confidentielle ou Information personnelle à CWT dans un délai de trente (30) jours après une telle demande, et ce, sans frais supplémentaires pour CWT. Le Fournisseur devra restituer, ou selon le choix de CWT, détruire toutes les Informations confidentielles et les Informations personnelles, y compris les copies électroniques et les copies papier, suivant les dispositions du Contrat ou, si le cas n'est pas mentionné dans le Contrat, dans un délai de quatre-vingt-dix (90) jours après l'évènement qui se produit le premier parmi les suivants : (a) l'expiration ou la résiliation du Contrat, (b) la demande par CWT de restituer les Informations confidentielles et les Informations personnelles, ou (c) la date après laquelle le Fournisseur n'a plus besoin des Informations confidentielles et des Informations personnelles pour fournir les services et produits dans le cadre du Contrat.

17.2 Dans l'éventualité où CWT approuverait la destruction comme alternative à la restitution des Informations confidentielles et des Informations personnelles, certifier par écrit que la destruction entraîne l'impossibilité de retrouver et de récupérer les Informations confidentielles et les Informations personnelles. Détruire entièrement toutes les copies des Informations confidentielles et

des Informations personnelles de CWT dans tous les emplacements et tous les systèmes où des Informations confidentielles et des Informations personnelles sont stockées, y compris, et sans s'y limiter, par les Tierces parties du Fournisseur qui ont été agréés. Lesdites informations seront détruites conformément à une procédure de destruction complète normalisée du secteur telle que la DOD 5220.22M ou la Publication Spéciale 800-88 de NIST, ou en utilisant un produit de démagnétisation recommandé par le fabricant du système concerné. Avant ladite destruction, appliquer toute Mesure de Sécurité Technique et Organisationnelle qui s'applique afin de protéger la sécurité, le caractère privé et la confidentialité des Informations confidentielles et des Informations personnelles.

17.3 Éliminer toute Information confidentielle ou Information personnelle de sorte qu'il soit impossible de reconstituer les informations dans un format utilisable. Les documents papier, diapositives, microfilms et photos doivent être éliminés par déchiquetage transversal ou par combustion. Les documents contenant des Informations confidentielles et des Informations personnelles en attente de destruction doivent être stockés dans des conteneurs sécurisés et transportés par une tierce partie fiable.

18. Conservation

Le Fournisseur devra :

18.1 Valider les exigences de conservation appropriées auprès des contacts de CWT avant de faire l'acquisition de toute Information confidentielle ou Information personnelle, et ce conformément au cahier des charges ou au bon de commande.

18.2 Sécuriser les copies de sauvegarde des Informations confidentielles et des Informations personnelles qui ont été automatiquement créées par les services, systèmes, dispositifs ou supports du Fournisseur ou d'une tierce partie (« **Copies d'Archives** »). Sauf dispositions contraires dans le Contrat, détruire de façon sécurisée toutes les Copies d'archives des Informations confidentielles et des Informations personnelles en appliquant une procédure normalisée du secteur au moins aussi restrictive que la DOD 5220.22M ou la Publication Spéciale 800-88 de NIST, et ce, dans un délai de 90 jours civils après l'expiration ou la résiliation du Contrat, ou plus tôt si CWT en fait la demande suivant des conditions raisonnables.

19. Réponse aux incidents et notification

Le Fournisseur devra :

19.1 Mettre en place et utiliser un processus de gestion des incidents et des procédures associées, et allouer les ressources spécialisées auxdits processus et procédures. Notifier immédiatement CWT, et au plus tard dans un délai de vingt-quatre (24) heures, de la survenue d'une attaque, d'une intrusion, d'un accès non autorisé, d'une perte ou d'un autre incident supposé ou confirmé concernant les informations, systèmes ou autres ressources de CWT.

19.2 Après avoir notifié CWT, fournir des mises à jour régulières du statut de l'incident, y compris, mais sans s'y limiter, des mesures prises pour résoudre l'incident en question, et ce, à intervalles ou aux moments convenus pendant la durée de l'incident, et dès que possible après la clôture de l'incident ; fournir un rapport écrit à CWT, détaillant l'incident, les mesures prises par le Fournisseur durant la réponse et les plans du Fournisseur pour de futures mesures en vue d'éviter qu'un incident similaire ne se reproduise.

19.3 Ne pas divulguer au public ladite violation d'information, de systèmes ou d'autres ressources de CWT sans en avoir informé CWT au préalable et sans avoir collaboré directement avec CWT pour informer les responsables du gouvernement à l'échelle locale, étatique, nationale ou régionale, les services de

surveillance de crédit applicables ou les personnes concernées par une telle violation et tout média qui convient, selon les exigences de la loi.

a. Mettre en place un processus pour permettre l'identification rapide de violations des contrôles de sécurité, y compris ceux qui sont stipulés dans les présentes Exigences concernant la Sécurité de l'Information commises par les employés du Fournisseur. Les employés du Fournisseur qui ont été ainsi identifiés feront l'objet de sanctions disciplinaires appropriées selon les lois qui s'appliquent. En dépit de ce qui précède, les employés du Fournisseur resteront sous l'autorité du Fournisseur. CWT ne sera pas considéré comme l'employeur des employés du Fournisseur.

20. Gestion de la **poursuite des activités et reprise des activités après un sinistre**

Le Fournisseur devra :

20.1 Développer, déployer, gérer et revoir ses plans de gestion de la continuité et de la reprise des activités après un sinistre afin de limiter l'impact sur CWT quant aux services et produits du Fournisseur. Les plans en question comprendront : les ressources désignées spécifiques aux fonctions de continuité et de reprise des activités après un sinistre, les objectifs de délai de reprise et les objectifs d'éléments de reprise qui ont été fixés, les sauvegardes quotidiennes de données et de systèmes, le stockage externe des supports et enregistrements de sauvegarde, la protection des enregistrements et les plans de contingence en fonction des exigences du Contrat, conserver les plans en question dans un endroit sécurisé en dehors des locaux et s'assurer que les plans sont mis à disposition du Fournisseur lorsque nécessaire.

20.2 Fournir, à la demande de CWT, un plan de continuité des activités documenté qui garantit que le Fournisseur peut remplir ses obligations en vertu du Contrat, y compris en vertu des exigences d'un cahier des charges ou d'un accord de niveau de service. Lesdits plans assureront la reprise des activités après un sinistre tout en protégeant l'intégrité et la confidentialité des Informations confidentielles et des Informations personnelles.

20.3 Mettre en place des procédures documentées pour la sauvegarde et la récupération sécurisées des Informations confidentielles et des Informations personnelles qui comprendront au minimum les procédures de transport, de stockage et d'élimination des copies de sauvegarde des Informations confidentielles et des Informations personnelles, et fournir à CWT lesdites procédures documentées lorsque CWT en fait la demande.

20.4 Faire en sorte que des sauvegardes de toutes les Informations confidentielles et les Informations personnelles stockées ou des logiciels et configurations des systèmes utilisés par CWT soient effectuées au moins une fois par semaine.

20.5 Mettre en pratique de façon complète et régulière, et ce, au moins une fois par an, ou suite à un changement substantiel dans la continuité des activités ou à des plans de reprise des activités dus à un sinistre, les plans en question aux seuls frais du Fournisseur. Les mises en pratique en question devront garantir le bon fonctionnement des technologies qui sont affectées et la bonne connaissance de ces plans en interne.

20.6 Vérifier dans les meilleurs délais les plans de continuité des activités pour faire face aux sources ou scénarios de risques supplémentaires ou émergents, et fournir à CWT un résumé général des plans et des tests, et ce, dans des délais raisonnables après que la demande en ait été faite.

20.7 S'assurer que tous les locaux du Fournisseur, ou contractés par le Fournisseur, qui hébergent ou traitent les Informations confidentielles et les Informations personnelles sont surveillés 24h/24, 7j/7 contre les risques d'intrusion, d'incendie, d'inondations et autres risques environnementaux.

21. Conformité et accréditation

Le Fournisseur devra :

21.1 Conserver des documents complets et exacts concernant le respect de ses obligations en vertu des présentes Exigences de Sécurité de l'Information, sous une forme permettant une évaluation ou un audit, et ce, pendant une période d'au moins trois (3) ans ou plus selon ce qui est requis suite à l'injonction d'un tribunal ou de poursuites civiles ou règlementaires. En dépit de ce qui précède, le Fournisseur n'aura l'obligation de conserver des journaux de sécurité que pour un minimum de six (6) mois après l'exécution continue du Contrat.

21.2 CWT peut, sans frais supplémentaires pour CWT et selon un préavis raisonnable, réaliser des évaluations ou des audits de sécurité réguliers des Mesures de Sécurité Techniques et Opérationnelles utilisées par le Fournisseur, durant lesquels CWT fournira au Fournisseur des questionnaires écrits et des demandes de documentation. Pour toute demande, le Fournisseur répondra d'autre part par écrit et en fournissant des justificatifs, le cas échéant, et ce, immédiatement ou après un accord mutuel. Suite à la demande de CWT pour un audit par CWT, le Fournisseur devra prévoir un audit de sécurité dans les dix (10) jours ouvrables qui suivent une telle demande. CWT pourra demander à avoir accès aux installations, systèmes, processus ou procédures afin d'évaluer l'environnement de contrôle de sécurité du Fournisseur.

21.3 À la demande de CWT, fournir la preuve de sa conformité aux conditions de ce document, et également vis-à-vis des certifications pour les dernières version de PCI-DSS, ISO 27001/27002, SOC 2, ou autre évaluation similaire pour le Fournisseur. Si le Fournisseur est dans l'incapacité de confirmer sa mise en conformité, il devra fournir un rapport écrit précisant en quoi il n'est pas en conformité et détaillant les mesures correctives envisagées pour être en conformité.

21.4 Dans l'éventualité où CWT estime, à sa seule discrétion, qu'il s'est produit une atteinte à la sécurité qui n'a pas été signalée à CWT conformément au présent document et aux Processus de Gestion d'Incidents du Fournisseur, prévoir un audit ou une évaluation qui commencera dans les vingt-quatre (24) heures suivant la notification par CWT d'une demande d'évaluation ou d'audit.

21.5 Fournir un rapport écrit à CWT dans les trente (30) jours civils suivant les résultats de l'évaluation ou du rapport d'audit, en insistant sur les mesures correctives que le Fournisseur a mises en place, ou qu'il propose de mettre en place, ainsi que l'échéancier et le statut actuel de chaque mesure corrective. Tous les trente (30) jours civils, transmettre à CWT un rapport actualisé rapportant le statut de toutes les mesures correctives jusqu'à la date de mise en œuvre. Mettre en œuvre toutes les mesures correctives dans les quatre-vingt-dix (90) jours qui suivent la réception du rapport d'évaluation ou d'audit, ou dans un délai alternatif, à condition que ce délai alternatif ait fait l'objet d'un accord mutuel par écrit entre les parties au plus tard trente (30) jours après la réception par le Fournisseur du rapport d'évaluation ou d'audit.

21.6 Déjà respecter et continuer de respecter les normes de sécurité de l'information et les exigences de rapport applicables rendues obligatoires par le gouvernement, et la norme ISO 27001/27002. Dans la mesure où il traite des numéros de compte de paiement ou toute autre information de paiement associée, devra déjà observer la version la plus récente de l'industrie des cartes de paiement (PCI-DSS) pour toute la gamme des systèmes qui traitent ces informations, et continuer de l'observer. Dans

l'éventualité où le Fournisseur ne serait plus en conformité avec les PCI-DSS concernant l'une des parties de la gamme complète des systèmes qui traitent les données applicables aux PCI, il devra en informer CWT dans les meilleurs délais, entreprendre immédiatement de remédier à son manquement sans délai injustifié et informer régulièrement CWT, à sa demande, du statut de cette rectification.

22. Normes, meilleures pratiques, règlementations et législation

Le Fournisseur devra :

Dans l'éventualité où le Fournisseur traiterait, accèderait, visionnerait, stockerait ou gèrerait des Informations confidentielles ou des Informations personnelles appartenant aux employés, associés, filiales, clients de CWT, ou des employés des clients, des entrepreneurs ou des sous-traitants de CWT, il appliquera des Mesures de Sécurité Techniques et Opérationnelles qui ne sont pas moins strictes que celles prévues par les principes, règlementations, directives et lois internationales, régionales, nationales, fédérales et locales qui s'appliquent.

23. Modification

CWT se réserve le droit de mettre à jour ou de modifier à tout moment les présentes Exigences de Sécurité de l'Information en en publiant la dernière version sur le site internet de CWT.

Version 2.0
Date : 15 Décembre 2017