MESURES TECHNIQUES ET ORGANISATIONNELLES

Sauf définition contraire ci-dessous, chaque terme défini dans ce document a la signification qui lui est attribuée dans le SDPA.

Les mesures techniques et organisationnelles du Fournisseur doivent comprendre, sans s'y limiter, les éléments suivants :

(i) **Organisation de la Sécurité de l'Information** – L'établissement, la mise en œuvre et le maintien de politiques de sécurité de l'information et d'un programme de Mesures Techniques et Organisationnelles de sécurité appropriées afin de protéger les Informations du Client, conformément aux Bonnes Pratiques du Secteur.

(ii) **Standards Sécurisés de Références** - Mesures visant à garantir que des configurations sécurisées pour les systèmes d'information soient élaborées, documentées et maintenues.

(iii) **Contrôles d'Accès** – Mesures d'accès au système et d'accès des utilisateurs et mesures d'authentification visant à empêcher l'accès aux Informations du Client de quelque manière ou à quelque fin que ce soit qui n'est pas autorisée par le Client ; ces mesures doivent inclure, sans s'y limiter, la prévention de l'entrée, de la lecture, de la copie, de la suppression, de la modification ou de la divulgation non autorisée des Informations du Client.

(iv) **Sécurité des Systèmes** - Mesures visant à renforcer les systèmes d'information et autres ressources conformément aux Bonnes Pratiques du Secteur.

(v) **Audit et Surveillance** - Mesures visant à maintenir une piste d'audit automatisée qui documente les événements liés à la sécurité des systèmes et tout événement de changement de gestion qui entraîne l'accès, la modification et/ou la suppression des Informations du Client.

(vi) **Sécurité des Réseaux** - Mesures visant à maintenir un processus formel de validation, de test et de documentation de toutes les connexions aux réseaux et de toutes les modifications apportées aux configurations des dispositifs des réseaux.

(vii) **Protection des Données** - Mesures visant à empêcher l'accès non autorisé, la modification ou la suppression des Informations du Client stockées ou en cours de transmission.

(viii) **Sensibilisation et formation à la sécurité** - Mesures visant à fournir une formation annuelle aux employés de manière régulière sur la sensibilisation à la sécurité, qui soit adaptée aux tendances, aux menaces et aux meilleures pratiques en matière de sécurité.

(ix) **Tests de Sécurité** - Mesures visant à identifier les vulnérabilités et à y remédier de manière régulière, conformément à la politique du Fournisseur, et à effectuer des tests de sécurité périodiques sur les systèmes et les applications ou lors de changements importants. Ces mesures doivent comprendre, sans s'y limiter, (1) l'engagement d'un tiers indépendant pour effectuer un audit de sécurité annuel sur tous les Systèmes du Fournisseur, (2) la réalisation de tests de pénétration réguliers et d'analyses de vulnérabilité hebdomadaires sur tous les Systèmes du

Fournisseur, (3) l'établissement et le maintien d'un programme de gestion des correctifs qui respecte ou surpasse les Bonnes Pratiques du Secteur, en vertu duquel le Fournisseur mettra régulièrement à jour et corrigera les logiciels susceptibles d'affecter directement ou indirectement les Informations du Client et/ou les Systèmes du Fournisseur et (4) la désignation, pour le Client, d'un agent de liaison en matière de sécurité qui sera disponible régulièrement pour discuter des Incidents de Sécurité de l'Information, des tests de sécurité, des résultats de sécurité et d'autres préoccupations en matière de sécurité. Si un manquement important est identifié à la suite de l'un des éléments ci-dessus ou d'une évaluation de sécurité menée par le Client, le Fournisseur remédiera à ce manquement important dans les 30 jours (tout manquement critique relevé qui n'est pas corrigé dans les 30 jours doit être immédiatement signalé au Client et, à la demande du Client, le Fournisseur fournira une attestation écrite que les tests de sécurité susmentionnés ont été effectués ainsi qu'une liste détaillée des vulnérabilités ouvertes et des plans de remédiation).

(x) **Contrôles de la Disponibilité -** Mesures visant à développer, exploiter, gérer et réviser les plans de continuité des activités et de reprise des activités après un sinistre, y compris la reprise technologique**.**

(xi) **Résolution des problèmes de sécurité des logiciels -** Si, dans le cadre des Services, le Fournisseur fournit des services SaaS ou PaaS ou tout autre service logiciel hébergé à distance, et si des vulnérabilités ou tout autre problème de sécurité sont découverts ou suspectés dans les logiciels par le Fournisseur ou le Client, les mesures liées aux corrections d'erreurs, mises à jour, correctifs, révisions, mises à niveau et nouvelles versions des logiciels (avec la documentation associée) inclus dans l'application mis à disposition du Client, dans le respect des délais ci-dessous. Le Fournisseur fournira au Client les preuves démontrant que tous les problèmes de sécurité identifiés ont été entièrement résolus conformément au plan d'action correctif établi.

Sévérité	Description	Prise en compte	Mises à jour	Résolution	Clôture
Urgent	Problèmes d'une ampleur catastrophique sans solution de contournement viable	1 heure ouvrable après la découverte d'une vulnérabilité ou d'un problème de sécurité	Toutes les 3 heures ouvrables	1 jour	7 jours
Critique	Problèmes qui constituent une menace sérieuse pour l'utilisateur final et/ou le Client	4 heures ouvrables après la découverte d'une vulnérabilité ou d'un problème de sécurité	Journalière	5 jours	14 jours
Important	Problèmes pour lesquels il existe une solution de contournement et qui peuvent être atténués par d'autres contrôles de sécurité en place	2 jours ouvrables après la découverte d'une vulnérabilité ou d'un problème de sécurité	5 jours	10 jours	45 jours
Non-critique	Tous les autres problèmes ou solutions de contournement	5 jours ouvrables après la découverte d'une vulnérabilité ou d'un problème de sécurité	5 jours	15 jours	Prochaine version