MESURES TECHNIQUES ET ORGANISATIONNELLES

(POUR LES FOURNISSEURS)

Ces Mesures techniques et organisationnelles (les « **MTO** ») font partie intégrante de l'Accord/Avenant/Pièce jointe/Programme/Section applicable relatif(ve) au Traitement des Données à caractère personnel (ou tout autre document équivalent, selon le cas) entre Avaya (y compris ses filiales internationales) et le Fournisseur (y compris ses filiales internationales, le cas échéant), qui les intègrent par renvoi.

1. Contrôle de l'accès aux locaux

Le Fournisseur doit prendre des mesures raisonnables afin d'empêcher l'accès physique à l'équipement de traitement des Données à caractère personnel par des personnes non autorisées comme suit :

1.1. Mettre en place un contrôle électronique de l'accès aux bâtiments abritant les Données à caractère personnel.

1.2. Mettre en place un contrôle électronique de l'accès aux zones sensibles dans les bâtiments, telles que les centres de données, les salles d'appel, les salles abritant le réseau local et les laboratoires.

1.3. Veiller à ce que les politiques soient en place en vue de s'assurer que seules les personnes autorisées peuvent accéder aux zones sensibles telles que les centres de données, les salles d'appel, les salles abritant le réseau local et tout autre endroit où des Données à caractère personnel sont traitées ou enregistrées. S'assurer que tous les droits d'accès à ces zones font l'objet d'une nouvelle validation chaque semestre.

1.4. Créer et conserver des journaux d'accès pendant une durée minimum de 90 jours.

1.5. S'assurer que les portes du périmètre et les zones sensibles sont surveillées et font l'objet d'une vidéosurveillance 24 heures/24 et 7 jours/7. Veiller à ce que l'ensemble des enregistrements de vidéosurveillance soient conservés pendant 30 jours au minimum.

1.6. Maintenir un système d'alarme surveillé de près, permettant de sécuriser les zones sensibles d'un point de vue physique (y compris les salles abritant le réseau local, les laboratoires et tout autre endroit dans lequel se déroule le traitement des Données à caractère personnel).

1.7. Veiller à ce que des agents de sécurité soient présents sur tout site de l'entreprise traitant des Données à caractère personnel.

1.8. Veiller à la mise en place d'un processus permettant de valider l'identité d'un individu avant d'attribuer un badge d'identification.

1.9. Les visiteurs doivent s'enregistrer et porter un badge permettant de les identifier facilement en tant que visiteurs. Les visiteurs doivent être accompagnés par le personnel pendant leur présence sur le site. L'ensemble des journaux relatifs aux visiteurs doit être conservé pendant un an au minimum.

1.10. Limiter et contrôler l'accès aux installations de stockage des supports et du centre de données abritant les Données à caractère personnel pour les prestataires externes, comme les agents de sécurité et les services d'entretien.

1.11. Conserver un programme de contrôle des clés documenté relatif à l'installation avec un journal pour la clé principale. Les clés des armoires, salles d'équipement et armoires de câblage doivent être maintenues sous bonne garde, fournies uniquement aux personnes autorisées, et leur retour doit être surveillé.

1.12. S'assurer que les enregistrements du contrôle d'accès sont vérifiés par l'administrateur responsable de l'activité d'alarme, y compris les alarmes concernant une porte restée ouverte ou une porte forcée.

2. Contrôle de l'accès à l'utilisation du système

Afin d'éviter tout accès logique à son équipement ou à ses applications de traitement des Données à caractère personnel par des personnes non autorisées, le Fournisseur doit prendre des mesures raisonnables afin de mettre en place et maintenir les mesures suivantes :

2.1. S'assurer qu'un identifiant unique est associé à chaque utilisateur d'un système (réseau, serveur, base de données, application).

2.2. S'assurer que l'octroi des comptes et des privilèges d'accès nécessite une validation par la direction et est vérifié tous les 6 mois.

2.3. Maintenir une liste de contrôle d'accès (LCA) pour l'ensemble des systèmes abritant des Données à caractère personnel et la contrôler régulièrement.

2.4. Pratiquer la règle du moindre privilège ainsi que le principe du « droit de savoir » lors de l'autorisation de l'accès aux utilisateurs.

2.5. Pratiquer la séparation des fonctions.

2.6. Veiller à la mise en place de processus destinés à suspendre les autorisations d'accès sous 24 heures pour les utilisateurs dont les fonctions chez le Fournisseur prennent fin (licenciement, mutation, etc.).

2.7. Désactiver les comptes utilisateur après 90 jours d'inactivité et les supprimer après 120 jours d'inactivité.

2.8. Veiller à ce que l'identité de chaque utilisateur soit vérifiée lorsque l'utilisateur tente de se connecter à l'aide de mots de passe, de l'authentification multi-facteurs ou de données biométriques. Les tentatives de connexion ayant réussi ou échoué doivent être enregistrées et conservées pendant 1 an.

2.9. Paramétrer un verrouillage automatique de l'écran par mot de passe après plus de 20 minutes d'inactivité.

2.10. Les mots de passe des utilisateurs doivent comporter au minimum 8 caractères, avec au moins un caractère appartenant à 3 catégories différentes sur les 4 (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux).

2.11. Les mots de passe de l'administrateur, au niveau du système et du compte de service doivent comporter au minimum 15 caractères, avec au moins un caractère de chaque catégorie sur les 4 (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux).

2.12. Les mots de passe doivent expirer tous les 90 jours.

2.13. Les nouveaux mots de passe doivent être différents des 10 derniers mots de passe.

2.14. Un compte doit se verrouiller automatiquement après 5 tentatives de connexion infructueuses.

2.15. L'ensemble des mots de passe par défaut du prestataire et de l'installation fournis avec le nouveau matériel, logiciel système et applications doivent être réinitialisés lors de l'installation.

2.16. Les mots de passe doivent être enregistrés et transmis dans un format crypté.

2.17. L'identifiant et le mot de passe temporaires initiaux doivent être communiqués de façon sûre. Les identifiant et mot de passe ne doivent jamais être envoyés en texte clair dans le même e-mail.

2.18. S'assurer que l'identité de l'utilisateur est validée avant d'autoriser la réinitialisation du mot de passe ou de fournir un mot de passe aux utilisateurs.

2.19. Standardiser la configuration et les versions du système d'exploitation et des serveurs conformément aux normes de l'industrie afin de les rendre résistants aux attaques.

2.20. Veiller à ce que les systèmes qui stockent ou traitent des Données à caractère personnel se trouvent sur un/des segment(s) de réseau(x) distinct(s) en fonction du libellé ou du niveau de classification des informations enregistrées sur les serveurs, afin de s'assurer que seules les personnes autorisées sont en mesure de communiquer avec les systèmes requis pour assumer leurs responsabilités spécifiques.

2.21. Maintenir un processus de gestion des correctifs documenté et réaliser des mises à jour sur les systèmes présentant des niveaux de vulnérabilité Critique et à Risque élevé sous 2 semaines après la publication du correctif, et sous un mois pour tous les autres. Appliquer également tout correctif sans attendre à la demande d'Avaya.

2.22. Le logiciel antivirus doit être chargé et opérationnel sur tous les serveurs et PC procédant au Traitement des Données à caractère personnel. Les Fournisseurs doivent utiliser d'autres techniques de détection des malwares lorsque cela est possible (par ex. scan des e-mails, scan du système de fichiers, scan du trafic Internet, etc.).

2.23. Le logiciel de scan antivirus doit être mis à jour au minimum quotidiennement, et doit être en mesure de prendre en charge des mises à jour de signatures urgentes en dehors de son cycle habituel.

2.24. Le logiciel antivirus doit être configuré de manière à ce que les utilisateurs non-privilégiés ne puissent pas le désactiver. Sous réserve des procédures de changement appropriées, les utilisateurs privilégiés peuvent désactiver le logiciel, lorsque ceci est adéquat.

3. Contrôle de l'accès aux Données à caractère personnel

Le Fournisseur doit prendre des mesures raisonnables afin d'empêcher tout accès logique aux Données à caractère personnel par des personnes non autorisées en mettant en place et en maintenant des mesures adéquates destinées à éviter toute lecture, copie, modification ou suppression non autorisées des supports contenant les Données à caractère personnel, tout enregistrement non autorisé dans la mémoire, toute lecture, modification ou suppression des Données à caractère personnel enregistrées. Cette protection sera assurée par les mesures suivantes :

3.1. Maintenir une politique de classification et de traitement des données écrite ainsi qu'un inventaire des documents avec une classification précisant l'emplacement physique et électronique.

3.2. Le Fournisseur doit veiller à ce que les Données à caractère personnel soient chiffrées en mouvement à l'aide de protocoles standards de l'industrie approuvés ; par ex. SSH/SCP/SFTPV2, TLS v1.2 ou supérieure.

3.3. Le Fournisseur doit assurer un niveau de chiffrement des Données à caractère personnel à la hauteur des normes de l'industrie et adapté aux risques présentés par le traitement des Données à caractère personnel statiques. L'ensemble des sauvegardes des Données à caractère personnel doivent toutefois être chiffrées sur des supports de sauvegarde.

3.4. Les Données à caractère personnel ne peuvent être téléchargées sur un PC, ordinateur portable, appareil mobile ou périphérique de stockage amovible de Fournisseur que si le chiffrement du disque dur est activé sur cet appareil.

3.5. Assurer la gestion et la rotation régulière de la clé de chiffrement.

3.6. Les Données à caractère personnel ne peuvent jamais être utilisées dans des environnements de développement, de test et/ou de mise en place, sauf si elles ont au préalable été pseudonymisées et une telle utilisation est autorisée par Avaya par écrit.

3.7. Si les informations de titulaires de cartes de crédit sont manipulées, enregistrées ou autrement traitées, les systèmes du Fournisseur doivent présenter la certification PCI DSS.

4. Contrôle de la transmission

Le Fournisseur doit prendre des mesures raisonnables pour empêcher toute modification et accès non autorisés aux Données à caractère personnel pendant la transmission, en mettant en place des canaux de communication sécurisés, et doit établir un enregistrement des transmissions comme suit :

4.1. S'assurer que les réseaux du périmètre sont séparés d'un point de vue physique ou logique des réseaux internes abritant des Données à caractère personnel.

4.2. Paramétrer des pare-feu entre : Internet et les systèmes tournés vers le Web ; les systèmes tournés vers le Web et les systèmes d'application ; les systèmes d'application et les réseaux internes. Ces pare-feu doivent être composés d'appareils physiquement distincts.

4.3. Utiliser des systèmes de détection d'intrusions sur réseau (NIDS) dans le cadre de la stratégie de sécurité du réseau en plus des pare-feu. L'ensemble des journaux NIDS doivent être vérifiés régulièrement afin de détecter toute tentative d'accès non autorisé aux Données à caractère personnel.

4.4. Les pare-feu doivent être utilisés dans le cadre d'une inspection d'état, et les règles du pare-feu doivent être révisées tous les ans.

4.5. Limiter et contrôler l'accès au réseau sans fil à l'aide de protocoles de sécurité sans fil standard de l'industrie, tout en veillant à maintenir un niveau WPA2 au minimum.

4.6. Limiter et contrôler l'accès au réseau à distance, et demander l'utilisation d'un VPN avec une authentification à deux facteurs.

5. Contrôle des saisies

Le Fournisseur doit prendre des mesures raisonnables afin de garantir la possibilité de vérifier et de déterminer si les Données à caractère personnel ont été ajoutées, modifiées ou supprimées de l'équipement de traitement des Données à caractère personnel, et la personne qui en est à l'origine, comme suit :

5.1. Chaque modification de configuration, sur les serveurs, des réseaux, des bases de données ou des applications commerciales utilisant des Données à caractère personnel ou la modification des Données à caractère personnel, doit être enregistrée. Les journaux d'audit doivent permettre de s'assurer que les actions peuvent être reliées à une personne, et doivent comprendre au minimum la date, l'heure et le type d'action. Les journaux d'audit doivent être conservés pendant 1 an.

5.2. Les journaux de contrôle d'accès, d'audit, de modification et d'événement doivent faire l'objet d'un contrôle actif. Ils doivent être vérifiés et rassemblés de façon centralisée pour tous les systèmes qui traitent ou contrôlent des Données à caractère personnel statiques et en mouvement à l'aide d'un mécanisme de collecte éprouvé de l'industrie, par ex. SIEM. Des alertes doivent être créées pour signaler tout accès non autorisé et toute anomalie. Les rapports relatifs aux anomalies et audits de journal doivent être fournis sur simple demande.

5.3. Maintenir une gestion de la configuration comprenant des paramètres de base sécurisés.

5.4. Établir une surveillance afin de détecter et de générer des alertes en cas de modification non autorisée.

5.5. S'assurer que les modifications d'urgence nécessitent une validation adéquate de la part de la direction avant leur mise en œuvre.

5.6. S'assurer que les conséquences en cas de violations de la politique sont mises en place, communiquées et appliquées.

6. Contrôle de l'organisation

Le Fournisseur doit prendre des mesures raisonnables pour ordonner l'organisation interne de manière à ce qu'elle soit conforme aux exigences spécifiques de la protection des données, ainsi que mettre en place et maintenir les mesures suivantes :

6.1. Maintenir une politique de sécurité des informations écrite, validée chaque année par l'équipe de direction du Fournisseur, et publiée et communiquée à l'ensemble des employés et tiers concernés du Fournisseur.

6.2. Maintenir une fonction de conformité et de sécurité dédiée afin de concevoir, de préserver et d'assurer la sécurité en soutien de sa « plateforme de confiance » et conformément aux normes de l'industrie. Cette fonction doit être axée sur l'intégrité du système, l'acceptation

des risques, l'analyse et l'évaluation des risques, l'estimation des risques, la gestion des risques et l'applicabilité de la solution ainsi que la gestion des fournisseurs.

6.3. Se soumettre à des contrôles de sécurité réguliers effectués par des tiers indépendants et fournir des rapports d'audits respectant les normes SSAE16 ou ISAE3402.

6.4. Recourir aux services de tiers indépendants reconnus dans l'industrie pour réaliser des évaluations concernant la vulnérabilité et des tests d'intrusion dans les réseaux, systèmes, applications et bases de données sur lesquels les Données à caractère personnel sont situées de façon statique, en mouvement et utilisées. Le Fournisseur doit catégoriser les vulnérabilités identifiées, et résoudre les vulnérabilités Critiques sous 4 semaines après la publication du correctif et les vulnérabilités à Risque élevé en conformité avec les standards de l'industrie généralement acceptés.

6.5. Maintenir le programme, les procédures et les outils de conformité, de protection des données et de sensibilisation à la sécurité destinés à traiter les menaces de sécurité des informations et à souligner les bonnes pratiques ; ainsi que les politiques, procédures et contrôles de sécurité des informations en place afin de protéger les Données à caractère personnel.

6.6. Maintenir, et à la demande d'Avaya lui fournir l'accès aux politiques, procédures et outils de rapport qui contiennent la documentation et les rapports correspondants sur la mise en œuvre, l'efficacité et la résolution, le cas échéant, des protections adéquates liées au traitement des Données à caractère personnel.

7. Contrôle de la disponibilité

Le Fournisseur doit prendre des mesures raisonnables afin d'éviter toute destruction ou perte accidentelles des Données à caractère personnel en mettant en place les mesures adéquates comme suit :

7.1. Surveiller les événements liés à la sécurité et paramétrer des notifications et des processus d'alerte sur l'ensemble des serveurs, des réseaux et des bases de données abritant des Données à caractère personnel.

7.2. Gérer un processus de réponse en cas d'incident de sécurité.

7.3. Maintenir des politiques, des procédures et des outils de planification d'urgence qui définissent les rôles et les responsabilités, et fournissent une direction claire ainsi qu'une formation sur la bonne gestion des événements imprévus, parmi lesquels se trouvent : les catastrophes naturelles, comme les inondations, tornades, séismes, ouragans et tempêtes de verglas ; les catastrophes accidentelles, comme les déversements chimiques ainsi que les défaillances électriques ou mécaniques ; et les actes délibérés comme les violations de sécurité et de confidentialité, les alertes à la bombe, les attaques et les vols.

7.4. Préserver la continuité de l'activité/mettre en place un plan de reprise des activités afin de restaurer les processus et opérations critiques pour les services du Fournisseur à/aux emplacement(s) depuis le(s)quel(s) les services du Fournisseur sont proposés. Le Fournisseur doit également disposer d'un plan testé chaque année afin de soutenir les opérations de manière planifiée et vérifiée en cas de catastrophe.

7.5. Conformément aux normes de l'industrie, mettre en place et maintenir un système d'alimentation de secours, des détecteurs de fumée et des alarmes incendie, des dispositifs d'extinction des incendies, des générateurs, des systèmes de refroidissement et un sol surélevé dans les centres de données qui traitent les Données à caractère personnel.

7.6. Réaliser des sauvegardes complètes de la/des base(s) de données abritant les Données à caractère personnel de façon sécurisée afin de garantir leur disponibilité en accord avec le degré d'importance des données.

8. Contrôle des actifs

Afin de garantir la protection de l'équipement ou des applications traitant des Données à caractère personnel, le Fournisseur doit prendre des mesures raisonnable afin de mettre en place et maintenir les mesures suivantes :

8.1. Veiller à la mise en place de procédures et d'outils afin d'identifier et de surveiller l'ensemble des équipements et des supports utilisés pour le traitement des Données à caractère personnel.

8.2. Attribuer la responsabilité de l'ensemble de l'équipement et des supports à un ou plusieurs gardiens.

8.3. Réaliser un contrôle annuel exhaustif de l'inventaire des actifs et une validation de l'inventaire des actifs pour en vérifier la précision, et identifier tout équipement et support manquant.

9. Contrôle des applications

Afin de garantir la protection des applications traitant des Données à caractère personnel, le Fournisseur doit mettre en place et maintenir les mesures suivantes :

9.1. Si applicable, en amont de la sortie de l'application, réaliser des tests d'intrusion et des tests afin de déterminer la vulnérabilité de l'application sur le Web et de réduire les vulnérabilités importantes en matière de sécurité.

9.2. Réaliser des tests d'intrusion au moins une fois par an dans son environnement informatique et fournir à Avaya les versions écrites des résultats de ces tests réalisés par le Fournisseur ou ses sous-traitants, au maximum 30 jours après que le Fournisseur a reçu les résultats ou les rapports.

9.3. Lorsque les applications (destinées à traiter les Données à caractère personnel) sont développées pour permettre au Fournisseur d'offrir des services à Avaya, s'assurer que les développeurs sont formés aux bonnes pratiques et aux standards de l'industrie du développement sécurisé.

9.4. Veiller à ce que les applications destinées à traiter les Données à caractère personnel sont développées de façon sécurisée à l'aide d'un processus formel du Fournisseur et documenté offrant la preuve de l'absence de vulnérabilités en matière de sécurité dans l'application avant qu'elle ne soit mise en production. Réaliser de nouveaux tests au moins chaque trimestre par la suite et après chaque modification importante. Les vulnérabilités en matière de sécurité des applications doivent au minimum intégrer celles répertoriées dans le SANS Top 20 et OWASP Top 10.

9.5. Les vulnérabilités en matière de sécurité des applications qui affectent les Données à caractère personnel doivent être corrigées dans un délai raisonnable après le moment où elles sont identifiées.

9.6. Ces exigences doivent être validées par des outils tels que le scan d'application dynamique et/ou l'analyse du code statique.

10. Modification et séparation du contrôle des données

Le Fournisseur doit mettre en place et maintenir les mesures de contrôle des modifications suivantes pour le traitement des Données à caractère personnel :

10.1. Maintenir les processus de gestion des modifications comprenant une documentation de l'objet, une analyse de l'impact sur la sécurité, un plan de test et ses résultats, ainsi qu'une autorisation de sa direction pour l'ensemble des modifications apportées aux systèmes qui traitent des Données à caractère personnel.

10.2. La configuration des systèmes qui traitent des Données à caractère personnel doit être validée avant la progression dans le réseau de production.

10.3. Toute modification apportée aux environnements de production abritant des Données à caractère personnel doit être contrôlée et validée par la direction du Fournisseur avec la mise à disposition de la documentation (contrôles/validations) dans le cas d'un audit.

10.4. Maintenir des environnements de développement, de test ou de mise en place séparés sur le plan physique et/ou logique par rapport aux environnements de production dans lesquels les Données à caractère personnel sont traitées.

10.5. Le Fournisseur doit conserver des bases de données séparées sur le plan physique et/ou logique pour le traitement des Données à caractère personnel d'Avaya.

- FIN DES MTO -