PHILIP MORRIS INTERNATIONAL

Sécurité des Informations

Terme	Définition
Actif:	signifie: (i) tout objet ou élément matériel, logiciel ou équipement qui est ou peut être utilisé afin de créer, accéder à, traiter, protéger, surveiller, conserver, extraire, afficher ou transmettre des données, de quelque nature qu'elles soient (y compris des données vocales); et (ii) tout document (quel qu'en soit le support) portant sur l'utilisation ou l'exploitation des objets et éléments susmentionnés.
Bonnes Pratiques de Sécurité:	signifient des mesures et pratiques conformes: (a) aux mesures et pratiques techniques et d'organisation qui sont exigées ou conseillées par les normes et codes internationaux de gestion et de bonnes pratiques en matière de Sécurité des Informations (tels qu'ISO/IEC 27001 (Systèmes de gestion de la sécurité des informations – exigences) et ISO/IEC 27002 (Code de bonnes pratiques relatif à la gestion de la sécurité de l'information)); et (b) aux normes et directives en matière de sécurité (y compris les principes généralement reconnus concernant la séparation des devoirs de gouvernance, de mise en œuvre, d'administration et de contrôle) et aux techniques telles que l'authentification rigoureuse, le contrôle d'accès, la vérification, l'attribution du « moindre privilège », telles que raisonnablement mises à la disposition du grand public ou des praticiens et parties prenantes dans le domaine de la sécurité des informations par des autorités et organisations généralement reconnues dans le domaine de la Sécurité des Informations, le cas échéant étendues, modifiées ou remplacées de temps à autre.
Client:	signifie la personne qui acquiert les Services dans le cadre du Contrat.
Contrat:	signifie le contrat entre le Client et le Prestataire qui incorpore cette annexe sur la sécurité des informations.
Données à Caractère Personnel:	signifie toute information qui concerne une Personne Concernée.
Données Client:	signifient les données: (a) que le Client, ou une personne agissant en son nom, fournit au Prestataire ou auxquelles il permet au Prestataire d'accéder, dans le cadre du Contrat; ou (b) que le Prestataire crée dans le cadre du Contrat.
Groupe Client:	signifie le Client et toutes ses Sociétés Affiliées. Au sens de la présente définition, un « membre du Groupe Client » désigne toute Société Affiliée du Client ou le Client lui-même.
Personne Concernée:	signifie toute personne physique ou morale identifiée ou identifiable; une « personne identifiable » est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs aspect(s) de son identité physique, physiologique, mentale, économique, culturelle ou sociale.
références au « **Personnel** »:	ces références incluent également les sous-traitants et les prestataires de la partie concernée.
Prestataire:	signifie la personne qui fournit les Services au Client dans le cadre du Contrat.
Sécurité des Informations:	signifie: (a) la protection et l'assurance: (i) de la confidentialité, l'intégrité, la fiabilité et la disponibilité des informations et des Systèmes; et (ii) des caractéristiques connexes des informations, telles que l'authenticité, la responsabilité et la non-répudiation; et (b) le respect de toutes les règlementations qui s'appliquent au Traitement des informations.
Services:	signifie les services qui sont fournis par le Prestataire dans le cadre du Contrat.

Société Affiliée:	signifie toute entité contrôlant une autre entité, contrôlée par une autre entité ou sous contrôle commun avec une autre entité; le terme « contrôler » et ses variantes signifient la capacité, directe ou indirecte, de diriger les affaires d'une autre entité en vertu d'un droit de propriété, d'un contrat ou de toute autre manière.
Système:	signifie un système, réseau, service ou solution informatique ou de communication (y compris tous les Actifs qui (a) en font partie ou qui (b) sont utilisés pour le fournir).
Système du Client:	signifie un Système auquel le Client (soit lui-même soit via un tiers) donne accès dans le cadre du Contrat.
Système du Prestataire:	signifie un Système auquel le Prestataire (soit lui-même soit via un tiers) donne accès dans le cadre du Contrat.
« **Traiter** » (et ses variations, telles que « Traitement »):	signifie la réalisation de toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication (par transmission, diffusion ou toute autre forme de mise à disposition), le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Le Prestataire doit:

(a) fournir les Services et exécuter ses obligations dans le cadre du Contrat conformément:

(i) à la présente annexe Sécurité des Informations; et

(ii) aux Bonnes Pratiques de Sécurité; et

(b) protéger les Services et les Données Client, notamment en mettant en œuvre les mesures techniques et d'organisation décrites dans le tableau ci-dessous (les « **Mesures de Sécurité** »).

Type de Mesure de Sécurité	**Détails des Mesures de Sécurité**
Respect des règlements internes:	1. Le Prestataire a établi, et doit appliquer et maintenir, des règlements internes qui: (a) obligent les employés à garder confidentielles les Données Client et à respecter les mesures techniques et d'organisation du Prestataire qui ont été établies afin de protéger les Données Client; et (b) règlent tout au moins les éléments suivants: (i) l'utilisation des ordinateurs, des appareils portables, du courrier électronique et de l'internet; et (ii) la manière de protéger les informations sur l'entreprise et les Données à Caractère Personnel. 2. Le Prestataire doit: (a) former ses employés et les tiers concernés (tels que les prestataires) à ces règlements et aux aspects connexes en matière de technologie de l'information et de sécurité; et (b) obliger ses employés, ainsi que les tiers concernés, à respecter ces règlements. Il est expressément demandé aux employés et aux prestataires de ne jamais partager ni noter des mots de passe.
Contrôles d'accès aux bâtiments:	S'agissant de ses bâtiments où des Données Client peuvent être Traitées, le Prestataire en contrôle l'accès notamment grâce: 1. à des cartes d'accès, des systèmes de vidéosurveillance ou d'autres formes de contrôles (y compris une combinaison de ces moyens); et 2. à des systèmes automatiques contrôlant les accès (et tentatives d'accès) et déclenchant des alarmes en cas d'accès non-autorisé ou de tentative d'accès non-autorisé. De plus, dans la mesure où le Prestataire conserve des Données Client ailleurs que directement sur les Systèmes du Client, le Prestataire doit s'assurer que des moyens automatisés sont en place s'agissant des sites où ces Données Client sont conservées de sorte à surveiller les conditions environnementales de ces sites et déclencher des alarmes dans le cas où ces conditions environnementales seraient inappropriées pour l'exploitation de systèmes informatiques (par exemple, en raison d'un incendie, de pannes de courant, d'inondations ou de variations de la température ou de l'hygrométrie requise).
Contrôles d'accès aux Systèmes	Le Prestataire doit: 1. Traiter les Données Client seulement (a) au moyen d'équipements (notamment des serveurs, postes de travail (par ex. des ordinateurs de bureau et portables) et d'équipements mobiles (par ex. des PDAs, smartphones, etc.)) qui sont sous le contrôle effectif du Prestataire; ou (b) dans le cadre

Type de Mesure de Sécurité	Détails des Mesures de Sécurité
utilisés par le Prestataire:	d'applications contrôlées par le Prestataire; et, dans ces deux cas, protéger de façon adéquate les Données Client qui sont conservées ou en cours de transmission; et 2. tenir une liste des emplacements des centres où son personnel Traite les Données Client placées sous son contrôle.
Contrôles de Systèmes et sécurité de l'infrastructure sous-jacente	S'agissant des Données Client que le Prestataire Traite au moyen d'un Système du Prestataire ainsi que des Données Client que le Prestataire Traite au moyen d'un Système du Client sur lequel il peut exercer un contrôle, le Prestataire doit: 1. limiter l'accès aux Systèmes qui contiennent les Données Client, notamment en: (a) restreignant le nombre de personnes bénéficiant d'un accès privilégié; (b) restreignant l'accès des utilisateurs aux seules parties du Système auquel ils ont besoin d'accéder pour effectuer leur travail; et (c) limitant la durée pendant laquelle ces personnes bénéficient de tels accès; 2. contrôler les droits d'accès utilisés par ou au nom du Prestataire pour accéder aux Systèmes du Client aussi souvent que cela est prévu par les règlements de sécurité du Prestataire, et dans tous les cas au moins une fois par année calendaire; 3. s'assurer que les membres du personnel qui ont accès aux Systèmes agissent de façon responsable et avec le soin qui s'impose; 4. tenir des listes de contrôle concernant l'accès aux systèmes de production ainsi que les permissions accordées sur des comptes utilisateur; 5. désactiver ou révoquer les droits d'accès des utilisateurs qui n'ont plus besoin de tels droits d'accès; 6. avoir un processus qui permette de s'assurer que les droits d'accès aux Systèmes du Prestataire ou à tout autre Système (p.ex. aux Systèmes du Client) auquel le Prestataire (soit lui-même soit par le biais d'un tiers) a accordé un accès soient révoqués lorsque le contrat de travail prend fin; 7. lorsque le Prestataire requiert un accès à ou des copies de Données Client dans le but de tester ou développer des logiciels, protéger les Données Client au moyen des mêmes restrictions d'accès aux systèmes que celles qui s'appliquent pour les Données Client dans les environnements de production; 8. respecter les conditions d'utilisation des ressources techniques et organisationnelles (concernant l'authentification et le contrôle des autorisations pour accéder aux systèmes informatiques ainsi que la gestion des comptes) qui sont nécessaires afin d'assurer la confidentialité, l'intégrité et la disponibilité des données Traitées; 9. s'assurer que les versions maîtres des Données Client sont exclusivement conservées sur les serveurs du réseau qui remplissent toutes les conditions suivantes: (i) ils sont effectivement contrôlés par le Prestataire; (ii) ils sont sécurisés; et (iii) des restrictions d'accès à ces serveurs ont été mises en place; et 10. installer et maintenir à jour une protection adéquate contre les logiciels malveillants. Le Prestataire doit contrôler l'accès aux Système du Prestataire: 11. s'agissant d'internet, en assurant la sécurité au moyen de pare-feu et d'autres mesures contre les demandes d'accès non-autorisées aux applications, sites ou services qui sont accessibles via l'internet, ou aux données d'accès qui sont communiquées via internet; 12. en limitant au personnel strictement autorisé l'accès aux fonctionnalités des systèmes (y compris les options de configuration du système informatique) ainsi qu'aux autres outils ayant trait à la sécurité des systèmes informatiques; 13. en installant de mesures de protection cryptographiques pour les données d'authentification (par ex. des mots de passe cryptés qui utilisent des algorithmes généralement sûrs reconnus dans l'industrie); 14. en allouant et retirant les identifiants et données d'accès des utilisateurs finaux; en activant une authentification et authentification unique pour lesquelles il est nécessaire de fournir un identifiant d'utilisateur et un mot de passe individuels et valables; 15. en appliquant les règles suivantes quant aux mots de passe: (a) les mots de passe doivent comprendre au moins huit caractères et au moins trois des quatre types de caractères suivants: (i) des lettres minuscules (de a à z); (ii) des lettres majuscules (de A à Z); (iii) des chiffres (de 0 à 9); et (iv) des caractères spéciaux (tels que !, $, #, %); et (b) les mots de passe doivent expirer automatiquement à des intervalles prédéterminés, un nouveau mot de passe devant alors être créé; 16. en désactivant automatiquement un identifiant d'utilisateur après cinq tentatives de connexion infructueuses;

Type de Mesure de Sécurité	Détails des Mesures de Sécurité
	17. en désactivant automatiquement chaque session après une période d'inactivité de 15 minutes au plus; 18. en gérant les droits des utilisateurs, identifiants et mots de passe. Le Client et le Prestataire peuvent, au cas par cas, convenir que les paragraphes **Error! Reference source not found.** à 16 ci-dessus ne s'appliqueront pas pour des parties de Systèmes qui ont pour vocation d'être publiquement accessibles. Dans la mesure où le Prestataire permet au Client de gérer lui-même les droits d'accès des utilisateurs, le Prestataire doit: 19. s'assurer que l'accès du Client aux Systèmes est sécurisé; et 20. fournir au Client des outils qui lui permettent d'exécuter les fonctions énoncées aux paragraphes **Error! Reference source not found.** à 18 ci-dessus.
Procédures de gestion de la sécurité interne:	Dans la mesure où le Prestataire Traite des Données Client autrement que directement sur les Systèmes d'Information du Client, le Prestataire a établi, et applique, des procédures de gestion de la sécurité interne qui recouvrent les aspects suivants: 1. la demande et l'autorisation de droits de traitement de données dans les Systèmes du Prestataire; l'octroi de ces droits dans les Systèmes; et l'identité de la personne qui est responsable de la demande, l'autorisation, l'octroi et la revue de ces droits; 2. les méthodes et ressources pour authentifier les utilisateurs des Systèmes, ainsi que les procédures de gestion et d'utilisation de ces méthodes et ressources; 3. la manière de créer et d'utiliser des copies des données du Système, des programmes et des programmes utilitaires qui sont utilisés pour sauvegarder et remettre en état les Systèmes, ainsi que de créer et de maintenir des données relatives aux Systèmes qui sont nécessaires pour vérifier et assurer la migration des Systèmes; 4. la protection appropriée de toute copie qui pourrait être nécessaire pour la sauvegarde ou l'archivage de Systèmes ou à d'autres fins; 5. la manière de sécuriser les Systèmes contre tout accès non-autorisé; 6. la manière dont les Systèmes enregistrent l'identité des personnes qui ont eu accès aux Systèmes, ainsi que la date et le périmètre des accès; 7. la manière d'évaluer et d'entretenir les Systèmes et supports qui sont utilisés pour le Traitement de données; 8. la manière de détruire en toute sécurité des informations qu'il n'est plus nécessaire de conserver; et 9. les procédures pour détecter et prévenir des incidents liés à la sécurité, y compris: (i) la gestion des actifs; (ii) l'évaluation de l'impact; et (iii) la mise en œuvre rapide de mesures correctives et la remontée des informations à toutes les parties appropriées.
Traitements des Données Client:	Dans la mesure où le Prestataire Traite des Données Client autrement que directement sur les Systèmes du Client, le Prestataire doit adopter et s'assurer du respect des procédures concernant la transmission et la protection d'informations et de Données Client. Entre autres, il doit: 1. adopter des lignes directrices pour la conservation et la destruction de la correspondance commerciale et d'autres documents; 2. adopter des règles qui régissent le téléchargement, l'utilisation et la conservation de logiciels et données de tiers; 3. s'assurer du respect de la sécurité informatique des Données Client qui sont transmises par voie électronique (que ce soit directement ou à travers d'outils de passage en production) entre Systèmes (qu'ils se trouvent chez le Prestataire ou dans les locaux d'autres parties); 4. gérer les supports amovibles et portables selon les Bonnes Pratiques de Sécurité et en particulier, s'il y a lieu: (a) les conserver dans un environnement sûr et sécurisé, conformément aux spécifications des fabricants; (b) les transporter, les supprimer et les détruire de façon sécurisée; et (c) conserver les supports de sauvegarde dans un site isolé se trouvant à une distance suffisante du site principal pour éviter des dommages en cas de sinistre affectant ce dernier; 5. protéger, par le biais de Bonnes Pratiques de Sécurité telles que le cryptage et les contrôles d'accès, les Données Client qui sont en cours de transmission et entreposées;

Type de Mesure de Sécurité	Détails des Mesures de Sécurité
	6. limiter l'accès aux Données Client aux membres du personnel qui doivent obligatoirement y avoir accès afin de fournir les Services, et veiller à ce que ces membres du personnel ne Traitent ces Données Client que dans la mesure nécessaire pour fournir les Services; 7. restituer au Client toutes les Données Client auxquelles le Prestataire n'a plus besoin d'avoir accès ou qui ne sont plus utilisées aux fins de prestation des Services; et 8. une fois que le Client a confirmé par écrit au Prestataire qu'il a bien reçu les Données Client qui lui ont été restituées conformément au paragraphe 7 ci-dessus, supprimer toutes les Données Client.
Gestion des Actifs:	Si le Prestataire est tenu de mettre hors service ou de détruire un Actif qui contient des Données Client, il doit garantir: 1. soit que l'Actif sera détruit de manière irréversible ou qu'il sera restitué au Client; 2. soit que les Données Client ou les informations pertinentes contenues dans l'Actif seront supprimées et rendues inexploitables avant que l'Actif ne soit mis hors service ou détruit.
Transmission:	1. Le Prestataire ne doit pas transmettre ou demander à un utilisateur de transmettre, via ou entre des Systèmes, des mots de passe en texte clair. 2. Le Prestataire ne doit pas transmettre, ni autoriser la transmission par un quelconque membre de son personnel de données non structurées de/au Client ou de/à l'un de ses Sociétés Affiliées, par un quelconque moyen autre que les Systèmes d'entreprise du Prestataire. En accord avec ce qui précède, le Prestataire ne doit pas utiliser ni permettre l'utilisation des moyens suivants pour l'hébergement ou la transmission de données non-structurées dans le cadre des Services, ou pour l'hébergement ou la transmission des Données Client: (a) des adresses électroniques autres que celles du Prestataire (par ex. Yahoo!, Gmail, etc.); (b) des protocoles de transfert de fichiers non sécurisés; ou (c) des services de partage de fichiers destinés au grand public. 3. Le Prestataire ne doit envoyer des supports CD/DVD/disque contenant des Données Client par courrier ou coursier à un quelconque destinataire (dont le Client et ses Sociétés Affiliées) qu'avec l'accord écrit préalable de l'interlocuteur chargé de la sécurité désigné par le Client. Si le Prestataire demande et reçoit cette autorisation, elle ne sera valable que pour la seule transmission en question.
Evaluation, rapports et information:	1. Le Prestataire doit prendre des mesures appropriées afin de vérifier: a) qu'il se trouve en conformité avec cette annexe; et b) que les mesures qu'il aura prises conformément à cette annexe sont suffisantes à la mise en œuvre des Bonnes Pratiques de Sécurité. 2. Dans la mesure où les activités du Prestataire dans le cadre du Contrat impliquent une solution en ligne ou sur un appareil mobile: (a) le Prestataire doit, au moins une fois par an, procéder à une évaluation de la sécurité (y compris des tests de performance) d'une telle solution en ligne ou sur appareil mobile et, sur demande, discuter des résultats avec le Client; et (b) le Client pourra lui-même, en coordination avec le Prestataire, procéder à une évaluation de la sécurité d'une telle solution en ligne ou sur appareil mobile. 3. Au moins une fois par trimestre (ou à tout autre intervalle auquel le Client aura consenti), le Prestataire doit fournir au Client des aperçus détaillés et facilement compréhensibles: (a) des autorisations d'accès délivrées aux personnes ayant accès aux Données Client; et (b) des traces d'audit de toutes les personnes ayant accès aux Données Client. 4. Le Prestataire doit informer le Client dans un délai raisonnable de la survenance chez le Prestataire d'un incident relatif à la sécurité ayant une incidence négative sur la confidentialité ou l'intégrité des Données Client.
Continuité du service:	Le Prestataire doit: 1. détecter, suivre, faire remonter et résoudre dans les meilleurs délais tout incident avéré (ou potentiel), toute défaillance, tout évènement affectant la sécurité et tout autre risque opérationnel; 2. tester, valider et mettre en œuvre toute modification des Systèmes du Prestataire d'une manière contrôlée afin de réduire autant que possible toute perturbation des activités du Client;

Type de Mesure de Sécurité	Détails des Mesures de Sécurité
	3. planifier, mettre en œuvre et tester régulièrement les mesures techniques et organisationnelles appropriées et nécessaires afin de maintenir ou de rétablir les services fournis au Client en cas d'événement perturbateur prévisible; et 4. garantir que tout site de secours ou alternatif utilisé pour assurer la continuité du service du Prestataire est soumis à des contrôles en matière de sécurité des informations au moins équivalents à ceux en vigueur sur le lieu sur lequel le Prestataire réalise habituellement les processus relocalisés.