SOUS-ANNEXE SECURITE SAAS

Introduction : Hyland maintient et gère un programme de sécurité complet, écrit, couvrant le Service Cloud Hyland et conçu pour protéger : (a) la sécurité et l'intégrité des Données Client ; (b) contre les menaces et les dangers pouvant avoir un impact négatif sur les Données Client ; et (c) contre les accès non autorisés aux Données Client. Le programme de sécurité comprend les éléments suivants :

I. Gestion des Risques.

a. Réalisation d'une évaluation annuelle des risques, conçue pour identifier les menaces et les vulnérabilités des mesures de protection administratives, physiques, légales, réglementaires et techniques utilisées pour protéger le Service Cloud Hyland.

b. Maintien d'un process documenté de remédiation des risques, afin d'attribuer la responsabilité des risques identifiés, d'établir les plans et délais de remédiation, et de prévoir un suivi périodique de l'avancement.

II. Programme de Sécurité de l'Information.

a. Maintien d'un programme de sécurité de l'information pour le Service Cloud Hyland, complet et documenté. Ce programme comprend des politiques et procédures établies à partir des pratiques standard de l'industrie, lesquelles peuvent inclure des normes ISO 27001/27002 ou équivalentes.

b. Ce programme de sécurité de l'information comprend, selon le cas : (i) la mise en œuvre de moyens de sécurité physique et de cyber-sécurité adéquats, là où les Données Client sont traitées et/ou stockées ; et (ii) la prise de précautions raisonnables en ce qui concerne les employés de Hyland.

c. Ces politiques seront revues et mises à jour chaque année par la direction d'Hyland.

III. Organisation de la Sécurité de l'Information. Attribution des responsabilités en matière de sécurité aux individus ou groupes Hyland appropriés afin de faciliter la protection du Service Cloud Hyland et des actifs associés.

IV. Sécurité des Ressources Humaines.

a. Les salariés de Hyland font l'objet d'un examen approfondi durant le process d'embauche. Des vérifications des antécédents et la validation des références sont effectuées afin de déterminer si les qualifications du candidat sont appropriées pour le poste proposé. Sous réserve de toute restriction imposée par la loi applicable et en fonction de la juridiction, ces vérifications d'antécédents comprennent la vérification du casier judiciaire, la validation des expériences professionnelles et la vérification des diplômes et formations, le cas échéant.

b. Hyland s'assure que tous ses salariés sont soumis à des engagements de confidentialité et de non-divulgation avant tout accès au Service Cloud Hyland ou aux Données Client.

c. Hyland s'assurer que tous les salariés concernés bénéficient d'une formation de sensibilisation à la sécurité dont l'objectif est de leur fournir les connaissances en matière de sécurité de l'information leur permettant d'assurer la sécurité, la disponibilité et la confidentialité des Données Client.

d. Lors du départ d'un salarié de Hyland ou d'un changement de poste, Hyland s'assure que tout accès salarié au Service Cloud d'Hyland est révoqué en temps utile et que tous les actifs de Hyland concernés, tant les informations que les équipements, lui sont

restitués.

V. Gestion des Actifs.

a. Maintien des politiques et procédures de gestion des actifs et des informations, en ce compris la propriété des actifs, leur inventaire, les lignes directrices pour leur classification et les normes de traitement relatives aux actifs Hyland.

b. Maintien des procédures de traitement des supports afin de garantir que les supports contenant des Données Client, dans le cadre du Service Cloud Hyland, sont cryptés et stockés dans un emplacement sécurisé soumis à des contrôles d'accès physiques stricts.

c. Lorsqu'un dispositif de stockage du Service Cloud Hyland a atteint la fin de sa durée de vie utile, les procédures visées par cet article comprennent un processus de mise hors service, appliquant les techniques recommandées par le *National Institute of Standards and technology* (le « NIST »), afin de détruire les données dans le cadre de process de mise hors service, conçu pour empêcher que les Données Client soient exposées à des personnes non autorisées.

d. Dans le cas où un dispositif de stockage Hyland ne pourrait pas être mis hors service par le biais des procédures visées ci-avant, ce dispositif est alors virtuellement déchiqueté, démagnétisé, purgé/essuyé ou physiquement détruit conformément aux pratiques courantes de l'industrie.

VI. Contrôles d'Accès.

a. Maintien d'une politique d'accès logique et de procédures correspondantes. Les procédures d'accès logique définissent le process de demande, d'approbation et de fourniture d'accès pour le personnel Hyland. Le process d'accès logique limite l'accès des utilisateurs Hyland (locaux et distants) selon leur fonction (basée sur le rôle/profil, accès approprié) pour les applications et les bases de données. La recertification de l'accès des utilisateurs Hyland afin de déterminer leurs accès et privilèges est effectuée périodiquement. Les procédures d'*onboarding* et d'*offboarding*, en temps utile, des utilisateurs du personnel Hyland seront documentées, de même que les procédures relatives au seuil d'inactivité des utilisateurs parmi le personnel de Hyland menant à la suspension et à la suppression de leur compte.

b. Limitation de l'accès de Hyland aux Données Client, à son personnel ayant à en connaître pour l'exécution des services fournis par Hyland en vertu du Contrat. Hyland a recours au principe du « moindre privilège » et au concept du « minimum nécessaire » afin de déterminer le niveau d'accès de ses utilisateurs aux Données Client. Hyland exige des mots de passe forts soumis à des exigences de complexité et à une rotation périodique, ainsi que l'utilisation d'une authentification multifactorielle.

c. Hyland s'assure que des contrôles d'accès stricts sont en place pour l'accès aux Données Client par Hyland. Les administrateurs du Client contrôlent l'accès de ses propres utilisateurs, leurs autorisations et la rétention des Données Client dans la mesure où de tels contrôles sont disponibles pour le Client en ce qui concerne le Service Cloud Hyland.

VII. Limites du Système.

a. Hyland n'encourt aucune responsabilité du fait des composants du système qui ne font pas partie de la Plateforme Cloud Hyland, en ce compris, les périphériques réseau, la connectivité réseau, les postes de travail, les serveurs et les logiciels détenus et exploités par le Client ou tiers. Hyland peut – à sa discrétion - fournir un support pour ces composants.

b. Les procédés auxquels il est fait recours au sein de la Plateforme Cloud Hyland sont limités à ceux qui sont exécutés par un salarié de Hyland (ou un tiers autorisé par Hyland) ou ceux qui sont exécutés dans les limites du système établi de Hyland, dans leur ensemble. Cela comprend, sans que cette liste soit exhaustive, l'installation de matériel(s), l'installation de logiciel(s), la réplication de données, la sécurité des données et les procédés d'authentification.

c. Nonobstant ce qui précède, certains procédés commerciaux peuvent s'affranchir de ces limites, dans la mesure où une ou plusieurs tâches sont exécutées hors des limites du système établi par Hyland pour la Plateforme Cloud Hyland, qu'elles soient réalisées par des individus n'étant pas des salariés de Hyland (ou des tiers autorisés par Hyland), ou qu'elles le soient sur le fondement de demandes écrites du Client. Dans un tel cas, Hyland fournit un support pour de tels procédés sous réserve qu'ils soient exécutés dans les limites du système établi de Hyland ; Hyland n'ayant aucune obligation de fournir un tel support dans le cas où les procédés sont exécutés en dehors des limites du système mis en place par Hyland. Hyland se réserve toutefois le droit, à sa discrétion, de fournir un support limité pour les procédés exécutés en dehors des limites de système établies pour la Plateforme Cloud Hyland. Les process commerciaux s'affranchissant des limites susvisées sont notamment, et sans que cette liste soit exhaustive, des changements de configuration du Service Cloud Hyland, des traitements réalisés dans le Service Cloud Hyland, l'autorisation de l'utilisateur et les transferts de fichiers.

VIII. Cryptage.

a. Les Données Client ne doivent être versées au Service Cloud Hyland que dans un format crypté, par exemple, de type SFTP, TLS/SSL, ou toute autre méthode équivalente.

b. Les Données Client doivent être cryptées durant leur stockage.

c. Lorsque l'utilisation de la fonctionnalité de cryptage est contrôlée ou modifiée par le Client, celui-ci en assume seul les risques associés.

IX. Sécurité Physique et de l'Environnement.

a. La Plateforme Cloud Hyland utilise des data centers ou des fournisseurs de services tiers qui ont démontré leur conformité avec une ou plusieurs des normes suivantes (ou objectivement similaires) : Organisation internationale de normalisation (« ISO ») 27001 et/ou rapports de *l'American Institute of Certified Public Accountants* (« AICPA ») sur les contrôles des organisations de services (« SOC »). Ces fournisseurs fournissent la connexion Internet, la sécurité physique, l'alimentation et les systèmes environnementaux ainsi que d'autres services pour la Plateforme Cloud Hyland.

b. Hyland utilise une architecture et des technologies conçues pour promouvoir à la fois la sécurité et une haute disponibilité.

X. Sécurité des Opérations.

a. Maintien de procédures d'exploitation documentées du cloud Hyland.

b. Maintien de contrôles de gestion des changements visant à s'assurer que les changements apportés aux systèmes de production du Service Cloud Hyland par Hyland sont correctement autorisés et examinés avant leur mise en œuvre. Le Client est seul responsable – avant toute utilisation du Service Cloud Hyland en mode production – de l'évaluation de tous changements de configuration, changements d'authentification et mises à niveau qu'il met en œuvre ou que Hyland met en œuvre à sa demande. Le Client peut, sous réserve d'une demande écrite (par exemple, par e-mail ou tout autre moyen de communication fourni par Hyland) adressée par l'un des Administrateurs de Sécurité du Client (un « ASC », tel que désigné par le Client ou au sein d'une Proposition de Services) et décrivant le(s) changement(s) attendu(s), solliciter Hyland afin qu'elle mette en œuvre celui/ceux-ci en son nom. Dans le cas où ceux-ci sont susceptibles d'impacter l'accès du Client au Service Cloud Hyland, Hyland effectue ces changements de configuration programmés pendant une fenêtre de maintenance planifiée. Dans les autres cas, Hyland se réserve le droit d'effectuer ces changements de configuration pendant les heures normales de travail.

c. Surveillance des niveaux d'utilisation et de capacité au sein de la Plateforme Cloud Hyland afin de planifier de manière adéquate et

proactive une augmentation future.

d. Utilisation de technologies de protection contre les virus et les logiciels malveillants, configurées pour répondre aux normes communes reconnues par l'industrie conçues pour protéger les Données Client et les équipements situés dans la Plateforme Cloud Hyland contre les attaques par virus ou tout autre charge associée à des programmes malveillants.

e. Mise en œuvre de plans de continuité et de reprise de l'activité après sinistre. Ceux-ci comprendront la réplication des Données Client sur un site secondaire.

f. Maintien d'un process de journalisation du système et de la sécurité afin de capturer les registres du système jugés critiques par Hyland. Ces registres sont conservés pendant au moins six (6) mois et examinés sur une base périodique.

g. Maintien des exigences de renforcement du système et des normes de configuration pour les composants déployés au sein de la Plateforme Cloud Hyland. Hyland s'assure que les serveurs, les systèmes d'exploitation et les logiciels de support utilisés dans la Plateforme Cloud Hyland reçoivent tous les correctifs de sécurité critiques et élevés en temps opportun, mais en aucun cas plus de quatre-vingt-dix (90) jours après leur publication, sous réserve de ce qui suit. Dans le cas où un correctif de sécurité, tel que susvisé, affecterait le Service Cloud Hyland de manière substantielle, Hyland s'efforce de mettre en œuvre des contrôles compensatoires dans l'attente de la disponibilité d'un correctif de sécurité n'affectant pas de manière substantielle le Service Cloud Hyland.

h. Réalisation de scans ou analyses de vulnérabilité de la Plateforme Cloud Hyland, a minima une (1) fois par trimestre, et réalisation d'opérations visant à remédier à toutes les vulnérabilités critiques et élevées identifiées conformément aux procédures de gestion des correctifs.

i. Réalisation de tests de pénétration de la Plateforme Hyland Cloud, a minima annuellement.

XI. Sécurité des Communications

a. Mise en œuvre de contrôles de sécurité de la Plateforme Hyland Cloud afin de protéger les ressources documentaires au sein de la Plateforme Hyland Cloud.

b. Lorsque cela est pris en charge, et lors de la mise en œuvre du Service Cloud Hyland, puis une (1) fois par période annuelle, le Client peut demander à Hyland de limiter l'accès au Service Cloud Hyland à une liste d'adresses IP prédéfinies, et ce sans frais supplémentaires.

XII. Relations Avec les Fournisseurs. Maintien d'un Programme de Gestion des Fournisseurs pour les fournisseurs critiques de Hyland. Ce programme garantit que les fournisseurs critiques sont évalués annuellement.

XIII. Incident de Sécurité.

a. Emploi des normes de réponse aux incidents basées sur les normes industrielles applicables, telles que ISO 27001:2013 et « National Institute for Standards and Technology » ("NIST »), afin de maintenir les composants de sécurité de l'information de l'environnement du Service Cloud Hyland.

b. Les réponses aux incidents susvisés suivent la procédure de réponse aux incidents documentée par Hyland, laquelle comprend la phase de déclenchement de l'incident, la phase d'évaluation, la phase d'escalade, la phase de réponse, la phase de récupération, la phase de désescalade et la phase d'examen post-incident.

c. Lorsque Hyland détermine que le Service Cloud Hyland du Client a été négativement impacté par un incident de sécurité, Hyland fournit un résumé de l'analyse des causes profondes de l'incident. La notification de ce résumé ne sera pas retardée de manière déraisonnable, mais n'interviendra qu'après la mise en place des actions correctives initiales visant à contenir la menace de sécurité

ou stabiliser le Service Cloud Hyland.

d. L'analyse des causes profondes de l'incident comprend la durée de l'événement, sa résolution, le résumé technique, les problèmes en suspens et le suivi, y compris les mesures que le Client doit prendre afin d'éviter d'autres problèmes. Les informations contenues dans le Service Cloud Hyland, en ce compris les données nécessitant des mesures de confidentialité et de sécurité additionnelles (en ce compris celles d'autres clients touchés par l'incident), ne sont pas divulguées publiquement. Le Client peut, s'il nécessite des détails supplémentaires sur un incident, en faire la demande à l'équipe de support Hyland GCS, laquelle est traitée au cas par cas. La procédure de divulgation d'informations peut nécessiter une évaluation sur site, afin de protéger la confidentialité et la sécurité des informations demandées.

e. Hyland notifie le Client d'un Incident de Sécurité dans les quarante-huit (48) heures. Un « Incident de Sécurité » désigne le cas où Hyland identifie une divulgation réelle de Données Client, non cryptées, à une personne ou entité non autorisée, et qui compromet la sécurité, la confidentialité ou l'intégrité des Données Client.

XIV. Aspects de la Gestion de la Continuité des Activités liés à la Sécurité de l'Information.

a. Maintien d'un plan de continuité de l'activité et de reprise après sinistre.

b. Révision et évaluation annuelle du plan susvisé.

XV. Données Agrégées.

a. Hyland est propriétaire de toutes les données d'enregistrement et de facturation du Client et de l'Utilisateur collectées et utilisées par Hyland, requises pour la configuration, l'utilisation du Service Cloud Hyland, ainsi que pour la facturation relative à ce dernier (les « Informations de Compte ») et de toutes les données agrégées, anonymisées et statistiques dérivées de l'utilisation et du fonctionnement du Service Cloud Hyland, en ce compris, mais sans s'y limiter, le nombre d'enregistrements dans le Service Cloud Hyland, le nombre et le type de transactions, les configurations , les rapports traités dans le cadre du Service Cloud Hyland, ainsi que les résultats de performance du Service Cloud Hyland (les « Données Agrégées »).

b. Hyland se réserve le droit d'utiliser les Informations de Compte et les Données Agrégées à des fins commerciales. Afin de lever toute ambiguïté, il est précisé que les Informations de Compte et les Données Agrégées ne comprennent pas les Données Client.

XVI. Enquêtes de Sécurité.

a. Contrôle de la conformité avec le programme de sécurité de l'information, constitué par des évaluations internes périodiques. Les résultats sont partagés avec la direction de Hyland et tout écart est suivi jusqu'à sa remédiation.

b. Maintien d'un programme d'audit externe périodique. Les attestations complètes, telles que les rapports SOC 2 disponibles, sont fournies - sur demande écrite – au Client.

c. Dans la limite d'une (1) fois par an (mais pas plus d'une fois au cours d'une période de 12 mois), le Client peut réaliser un audit (qui comprend des évaluations, des questionnaires, des revues guidées ou d'autres demandes de validation des contrôles de sécurité de Hyland) (chacun une « Enquête de Sécurité ») des opérations de Hyland dans le cadre de la fourniture et du support du Service Cloud Hyland auquel il a souscrit, sous réserve d'une notification préalable écrite à Hyland et des critères suivants à condition que le Client informe à l'avance Hyland de son désir de mener une telle Enquête de Sécurité et que l'Enquête de Sécurité proposée ne chevauche pas, ou couvrir autrement les mêmes informations ou des informations similaires que, ou portée de: (1) tout contrôle déjà prévu par un audit ou une évaluation externe déjà effectué par Hyland, tel qu'un rapport SOC 2, ISO 27001 ou tout autre audit ou évaluation similaire mis à la disposition du Client à la demande du Client; ou (2) tout contenu déjà fourni par Hyland via son SIG, CAIQ ou un

questionnaire similaire rempli qui est mis à la disposition du Client sur demande: (1) Hyland et le Client doivent s'entendre mutuellement sur le calendrier, la portée et les critères de cette Enquête de Sécurité, qui, sous réserve de ce qui précède, peut inclure l'achèvement des questionnaires fournis par le Client; (2) la documentation confidentielle et restreinte, telle que les politiques, pratiques et procédures internes de Hyland, y compris toute documentation demandée par le client qui ne peut pas être retirée des locaux de Hyland en raison de limitations physiques ou de restrictions de politique ne sera pas fournie à l'extérieur ou retirée des locaux de Hyland et de tels examens doit être effectuée sur place au siège social de Hyland dans l'Ohio ou par le biais d'une capture d'écran sécurisée qui peut être organisée par Hyland pour interdire tout type de copie ou de capture d'écran; (3) Le client comprend et accepte que Hyland ne permettra pas l'accès aux systèmes ou appareils internes utilisés pour héberger ou prendre en charge les offres de Hyland; (4) dans la mesure où le client souhaite engager un tiers pour effectuer une telle Enquête de Sécurité, Hyland doit approuver ce tiers par écrit à l'avance, Le client doit amener ce tiers à conclure un accord de non-divulgation avec Hyland et à accepter de respecter les normes de sécurité de Hyland, et le client doit gérer l'engagement avec le tiers, s'assurer que le tiers comprend la portée de l'Enquête de Sécurité comme convenu d'un commun accord entre Hyland et le client et comment le client utilise le service Hyland Cloud, et, et (b) le Client paiera à Hyland les montants requis par Hyland en lien avec les Prestations de Services (y compris les frais et dépenses remboursables) fournies dans le cadre d’ Enquête de Sécurité (aux tarifs publics de Hyland alors en vigueur). Le cas échéant, Hyland fournit dans une mesure raisonnable un accès privé au siège social de Hyland, Ohio, U.S., pour analyser des données et des réunions. Sous réserve d’un demande écrite préalable raisonnable, les parties peut conviennent de rendre disponible les salariés ou prestataires dont l’intervention est nécessaire en vue d’entretiens dans le cadre de réunions physiques ou par téléphone, pendant la durée de l’Enquête de Sécurité, ce, aux seuls frais du Client. Le Client s’interdit, et le client interdira chaque tiers Enquête de Sécurité de distribuer ou de publier les résultats de l’ Enquête de Sécurité à tout tiers, sans le consentement préalable écrit de Hyland. Nonobstant toute disposition contraire de la présente entente, rien dans la présente entente (, y compris cette section), n'obligera Hyland ou l'une de ses sociétés affiliées à divulguer des informations soumises au privilège avocat-client.