APÊNDICE DE SEGURANÇA DE SAAS

Introdução: A Hyland mantém e gerencia um programa abrangente de segurança por escrito para cobertura do Serviço de Nuvem da Hyland projetado para proteger: (a) a segurança e integridade dos Dados do Cliente; (b) contra ameaças e perigos que possam afetar negativamente os Dados do Cliente; e (c) contra acesso não autorizado aos Dados do Cliente, cujo programa inclui o seguinte:

I. Gestão de Riscos

a. Realização de uma avaliação de risco anual projetada para identificar ameaças e vulnerabilidades nas medidas de segurança administrativas, físicas, legais, regulatórias e técnicas usadas para proteger o Serviço de Nuvem da Hyland.

b. Manutenção de um processo de correção de riscos documentado para atribuir a propriedade dos riscos identificados, estabelecer planos e prazos de correção e fornecer monitoramento periódico do progresso.

II. Programa de Segurança de Informações

a. Manutenção de um programa abrangente e documentado de segurança da informação do Serviço de Nuvem da Hyland. Este programa incluirá políticas e procedimentos baseados em práticas padrões do setor, as quais podem incluir ISO 27001/27002, ou outro padrão equivalente.

b. Esse programa de segurança da informação deve incluir, conforme aplicável: (i) segurança física e cibernética adequada onde os Dados do Cliente serão tratados e/ou armazenados; e (ii) precauções razoáveis tomadas com relação ao emprego de pessoal da Hyland.

c. Essas políticas serão revisadas e atualizadas pela gerência da Hyland anualmente.

III. Organização da Segurança da Informação.

Atribuição de responsabilidades de segurança a indivíduos ou grupos da Hyland apropriados para facilitar a proteção do Serviço de Nuvem da Hyland e dos ativos associados.

IV. Segurança de Recursos Humanos

a. Os empregados da Hyland são submetidos a uma triagem abrangente durante o processo de contratação. Verificações de antecedentes e validação de referência serão realizadas para determinar se as qualificações dos candidatos são apropriadas para o cargo proposto. Sujeitas a quaisquer restrições impostas pela lei aplicável e com base na jurisdição, essas verificações de antecedentes incluem verificações de antecedentes criminais, validação para o emprego e verificação educacional.

b. Garantia de que todos os empregados da Hyland estejam sujeitos a compromissos de confidencialidade e não divulgação antes que seja fornecido o acesso ao Serviço de Nuvem da Hyland ou Dados do Cliente.

c. Garantia de que os empregados aplicáveis da Hyland recebam treinamento de conscientização sobre segurança, projetado para fornecer a esses empregados conhecimentos sobre segurança da informação para garantir a segurança, disponibilidade e confidencialidade dos Dados do Cliente.

d. Após a separação ou alteração de funções dos empregados da Hyland, a Hyland garantirá que qualquer acesso dos empregados da Hyland ao Serviço de Nuvem da Hyland seja revogado em tempo hábil e que todos os ativos aplicáveis da Hyland, tanto informações quanto físicos, sejam devolvidos.

V. Gestão de Ativos

a. Manutenção de políticas e procedimentos de gerenciamento de ativos e informações. Isso inclui a propriedade de ativos, um

inventário de ativos, diretrizes de classificação e padrões de manuseio referentes aos ativos da Hyland.

b. Manutenção dos procedimentos de manipulação de mídia para garantir que a mídia que contém Dados do Cliente como parte do Serviço de Nuvem da Hyland seja criptografada e armazenada em um local seguro, sujeito a rígidos controles de acesso físico.

c. Quando um dispositivo de armazenamento da Hyland chega ao fim de sua vida útil, os procedimentos incluem um processo de descomissionamento projetado para impedir que os Dados do Cliente sejam expostos a pessoas não autorizadas, usando as técnicas recomendadas pelo NIST para destruir dados como parte do processo de descomissionamento.

d. Se um dispositivo de armazenamento do Serviço de Nuvem da Hyland não puder ser descomissionado usando esses procedimentos, o dispositivo será virtualmente fragmentado, desmagnetizado, eliminado/limpo ou destruído fisicamente, de acordo com as práticas padrão do setor.

VI. Controles de Acesso

a. Manutenção de uma política de acesso lógico e dos procedimentos correspondentes. Os procedimentos de acesso lógico definirão o processo de solicitação, aprovação e fornecimento de acesso para o pessoal da Hyland. O processo de acesso lógico restringirá o acesso do usuário da Hyland (local e remoto) com base na função de trabalho do usuário da Hyland (com base na função/perfil, acesso apropriado) para aplicativos e bancos de dados. A recertificação de acesso de usuário da Hyland para determinar o acesso e os privilégios será realizada periodicamente. Os procedimentos para integração e exclusão de usuários da Hyland em tempo hábil serão documentados. Os procedimentos para o limite de inatividade do usuário pessoal da Hyland, levando ao limite de suspensão e remoção da conta, serão documentados.

b. Limitação de acesso da Hyland aos Dados do Cliente ao seu pessoal que precisa acessar os Dados do Cliente como uma condição para o desempenho pela Hyland dos serviços sob este Contrato. A Hyland deve utilizar o princípio de "privilégio mínimo" e o conceito de "mínimo necessário" ao determinar o nível de acesso de todos os usuários da Hyland aos Dados do Cliente. A Hyland exigirá senhas fortes, sujeitas a requisitos de complexidade e rotação periódica, e o uso de autenticação multifator.

c. Garantia de controles rígidos de acesso para o acesso aos Dados do Cliente pela Hyland. Os administradores do Cliente controlam o acesso do seu usuário, as permissões do usuário e a retenção de Dados do Cliente na medida em que tais controles estejam disponíveis para o Cliente em relação ao Serviço de Nuvem da Hyland.

VII. Limites do Sistema

a. A Hyland não é responsável por nenhum componente do sistema que não esteja dentro da Plataforma de Nuvem da Hyland, incluindo dispositivos de rede, conectividade de rede, estações de trabalho, servidores e software detidos e operados pelo Cliente ou por terceiros. A Hyland pode fornecer suporte para esses componentes a seu critério razoável.

b. Os processos executados dentro da Plataforma de Nuvem da Hyland são limitados àqueles executados por um funcionário da Hyland (ou terceiros autorizados pela Hyland) ou processos executados dentro dos limites de sistema estabelecidos pela Hyland, no conjunto. Isto inclui, mas não está limitado a, instalação de hardware, instalação de software, replicação de dados, segurança de dados e processos de autenticação.

c. Certos processos comerciais podem ultrapassar estes limites, o que significa que uma ou mais tarefas são executadas fora dos limites de sistema estabelecidos pela Hyland para a Plataforma de Nuvem da Hyland, uma ou mais tarefas são executadas por indivíduos que não são funcionários da Hyland (ou terceiros autorizados), ou uma ou mais tarefas são executadas com base em solicitações por escrito feitas pelo Cliente. Em tal caso, a Hyland dará suporte a tais processos na medida em que eles ocorram dentro dos limites de sistema estabelecidos pela Hyland, mas a Hyland não será responsável por fornecer suporte a tais processos na medida em que eles ocorram fora dos limites de sistema estabelecidos. A seu critério razoável, a Hyland poderá fornecer suporte limitado para processos que ocorram fora dos limites de sistema estabelecidos para a Plataforma de Nuvem da Hyland. Exemplos de processos comerciais que ultrapassam esses limites incluem, mas não estão limitados a, mudanças na configuração do Serviço de Nuvem da Hyland, processamento que ocorra dentro do Serviço de Nuvem da Hyland, autorização de usuário e transferências de arquivos.

VIII. Criptografia

a. Os Dados do Cliente somente deverão ser carregados no Serviço de Nuvem da Hyland em formato criptografado como SFTP,

TLS/SSL, ou outro método equivalente.

b. Os Dados do Cliente deverão ser criptografados em repouso.

c. Onde o uso da funcionalidade de criptografia pode ser controlado ou modificado pelo Cliente, caso o Cliente decida modificar o uso ou desativar qualquer funcionalidade de criptografia, o Cliente o fará por seu próprio risco.

IX. Segurança física e do Ambiente

a. A Plataforma de Nuvem da Hyland utiliza centros de dados ou provedores serviço terceirizados que tenham demonstrado conformidade com um ou mais dos seguintes padrões (ou um equivalente razoável): *International Organization for Standardization* ou Organização Internacional para Padronização ("ISO") 27001 e/ou *American Institute of Certified Public Accountants* ou Instituto Americano de Contadores Públicos Certificados ("AICPA") Relatórios para Organizações de Serviços do *Service Organization Controls* ou Controles de Organização de Serviço ("SOC"). Esses provedores fornecem conectividade com a Internet, segurança física, energia e sistemas de ambiente e outros serviços para a Plataforma de Nuvem da Hyland.

b. A Hyland usa arquitetura e tecnologias projetadas para promover tanto a segurança quanto a alta disponibilidade.

X. Segurança de Operações

a. Manutenção dos procedimentos operacionais da nuvem da Hyland documentados.

b. Manutenção dos controles de gerenciamento de alterações para garantir que as alterações nos sistemas de produção do Serviço de Nuvem da Hyland feitas pela Hyland sejam devidamente autorizadas e revisadas antes da implementação. O Cliente é responsável por testar todas as alterações de configuração, autenticação e atualizações implementadas pelo Cliente ou implementadas pela Hyland a pedido do Cliente antes do uso em produção do Serviço de Nuvem da Hyland. Nos casos em que o Cliente confia na Hyland para implementar alterações em seu nome, uma solicitação por escrito descrevendo a alteração deve ser enviada (por exemplo, um e-mail ou outro método fornecido pela Hyland) pelos Administradores de Segurança do Cliente ou *Customer Security Administrators* ("CSAs") designados pelo Cliente ou descrita em uma Proposta de Serviços. A Hyland fará alterações agendadas na configuração que deverão impactar o acesso do Cliente ao seu Serviço de Nuvem da Hyland durante uma janela de manutenção planejada. A Hyland pode fazer alterações na configuração que não devem impactar o Cliente durante o horário comercial normal.

c. Monitoramento dos níveis de uso e capacidade na Plataforma de Nuvem da Hyland para planejar de forma adequada e proativa o crescimento futuro.

d. Utilização de tecnologias de proteção contra vírus e *malware*, configurados para atender aos padrões comuns do setor, projetados para proteger os Dados e equipamentos do Cliente localizados na Plataforma de Nuvem da Hyland contra infecções por vírus ou cargas mal-intencionadas semelhantes.

e. Implementação de procedimentos de recuperação de desastres e continuidade de negócios. Isso incluirá a replicação dos Dados do Cliente em um local secundário.

f. Manutenção de um sistema e de um processo de registro de segurança para capturar registros do sistema considerados crítico pela Hyland. Esses registros devem ser mantidos por pelo menos seis meses e revisados periodicamente.

g. Manutenção dos requisitos de proteção do sistema e dos padrões de configuração para componentes implantados na Plataforma de Nuvem da Hyland. Garantia de que servidores, sistemas operacionais e software de suporte usados na Plataforma de Nuvem da Hyland recebam todos os patches críticos e de alta segurança em tempo hábil, mas em nenhum caso mais de 90 dias após o lançamento, sujeito à próxima frase. Caso qualquer patch de segurança afete substancialmente o Serviço de Nuvem da Hyland, a Hyland envidará esforços razoáveis para implementar controles compensadores até que esteja disponível um patch de segurança que não afete substancialmente o Serviço de Nuvem da Hyland.

h. Realização de varreduras ou análise de vulnerabilidades da Plataforma de Nuvem da Hyland pelo menos trimestralmente e remediação de todas as vulnerabilidades críticas e altas identificadas de acordo com seus procedimentos de gestão do patch.

i. Realização de testes de penetração na Plataforma de Nuvem da Hyland pelo menos anualmente.

XI. Segurança de Comunicações

a. Implementação de controles de segurança na Plataforma de Nuvem da Hyland para proteger recursos de informações na Plataforma de Nuvem da Hyland.

b. Quando suportado, após a implementação, e pelo menos uma vez por ano após a implementação, o Cliente pode solicitar à Hyland que limite o acesso ao Serviço de Nuvem da Hyland do Cliente a uma lista de endereços IP predefinidos, sem nenhum custo adicional.

XII. Relações com Fornecedores. Manutenção de um Programa de Gestão de Fornecedores para seus fornecedores críticos. Este programa garantirá que os fornecedores críticos sejam avaliados anualmente.

XIII. Incidente de Segurança

a. Emprego de padrões de resposta a incidentes baseados em padrões aplicáveis do setor, como ISO 27001:2013 e Instituto Nacional de Padrões e Tecnologia ("NIST"), para manter os componentes de segurança da informação do ambiente do Serviço de Nuvem da Hyland.

b. As respostas a esses incidentes seguem a sequência de resposta de incidentes documentada da Hyland. Essa sequência inclui a fase de acionamento do incidente, fase de avaliação, fase de progressão, fase de resposta, fase de recuperação, fase de regressão e fase de revisão pós-incidente.

c. Se a Hyland determinar que o Serviço de Nuvem da Hyland do Cliente foi impactada negativamente por um incidente de segurança, a Hyland entregará um resumo da análise de causa raiz. Esse aviso não será injustificadamente atrasado, mas ocorrerá após as ações corretivas iniciais terem sido tomadas para conter a ameaça à segurança ou estabilizar a Plataforma de Nuvem da Hyland.

d. A análise da causa raiz incluirá a duração do evento, a resolução, o resumo técnico, os problemas pendentes e o acompanhamento, incluindo as etapas que o Cliente precisa executar para evitar novos problemas. As informações do Serviço de Nuvem do Cliente, incluindo elementos de dados que exigem medidas adicionais de confidencialidade e segurança (incluindo as de outros clientes afetados no evento), não serão divulgadas publicamente. Se o Cliente precisar de detalhes adicionais de um incidente, uma solicitação à equipe de Suporte de GCS da Hyland deve ser enviada e tratada caso a caso. O processo de liberação das informações pode exigir uma revisão no local para proteger a confidencialidade e a segurança das informações solicitadas.

e. A Hyland notificará o Cliente sobre um Incidente de Segurança dentro de 48 horas. Um "Incidente de Segurança" significa uma determinação pela Hyland de uma divulgação real de Dados do Cliente não criptografados a uma pessoa ou entidade não autorizada que comprometa a segurança, confidencialidade ou integridade dos Dados do Cliente.

XIV. Aspectos de Segurança da Informação da Gestão de Continuidade de Negócios

a. Manutenção de um plano de continuidade de negócios e recuperação de desastres.

b. Revisão de teste deste plano anualmente.

XV. Dados Agregados

a. A Hyland é proprietária de todos os dados de registro e faturamento de Clientes e Usuários coletados e utilizados pela Hyland que são necessários para a configuração, uso e faturamento do Serviço de Nuvem da Hyland (“Informações de Conta”) e todos os dados agregados, anônimos e estatísticos derivados do uso e da operação do Serviço de Nuvem da Hyland, incluindo, sem limitação, o número de registros no Serviço de Nuvem da Hyland, o número e os tipos de transações, configurações e relatórios processados como parte do Serviço de Nuvem da Hyland e os resultados de desempenho do Serviço de Nuvem da Hyland (os “Dados Agregados").

b. A Hyland poderá utilizar as Informações de Conta e Dados Agregados para fins de operação dos negócios da Hyland. Para maior clareza, as Informações de Conta e os Dados Agregados não incluem Dados do Cliente.

XVI. Testes de Segurança e Auditoria

a. Monitoramento de sua conformidade com seu programa de segurança da informação. Isso inclui revisões internas periódicas. Os resultados são compartilhados com a liderança da Hyland e os desvios são rastreados até a correção.

b. Manutenção de um programa periódico de auditoria externa. As certificações concluídas, como relatório SOC 2 mais recente da Hyland disponível, serão fornecidos para os Clientes mediante solicitação por escrito.

c. O Cliente pode realizar auditorias das operações da Hyland que participam da entrega e suporte contínuos do Serviço de Nuvem da Hyland adquirido pelo Cliente anualmente; contanto que o Cliente forneça à Hyland uma notificação por escrito de seu desejo de realizar tal auditoria e os seguintes critérios sejam atendidos: (a) a Hyland e o Cliente concordem mutuamente com o prazo, o escopo e os critérios de tal auditoria, que podem incluir o preenchimento de questionários fornecidos pelo Cliente e a revisão guiada de políticas, práticas, procedimentos, configurações do Serviço de Nuvem da Hyland, faturas ou registros de aplicativos, e (b) o Cliente concorde pagar as taxas d Hyland (às taxas padrão da Hyland) pelos Serviços Profissionais exigidos ou solicitados da Hyland em conexão com essa auditoria. Antes de qualquer auditoria, qualquer terceiro contratado pelo Cliente para auxiliá-lo deve ser instruído pela Hyland e assinar um Contrato de Não Divulgação diretamente com a Hyland. Se qualquer documentação solicitada pelo Cliente não puder ser removida das instalações da Hyland como resultado de limitações físicas ou restrições políticas, a Hyland permitirá que os auditores do Cliente acessem essa documentação na sede corporativa da Hyland em Ohio e pode proibir qualquer tipo de cópia ou captura de tela. Quando necessário, a Hyland fornecerá acomodações privadas e razoáveis na sede corporativa da Hyland em Ohio para análise de dados e reuniões. Mediante aviso razoável, a Hyland e o Cliente concordam mutuamente em disponibilizar os empregados ou contratados necessários para entrevistas pessoalmente ou por telefone durante essa auditoria, ao custo e despesa do Cliente. É proibido ao Cliente distribuir ou publicar os resultados dessa auditoria a terceiros sem a aprovação prévia por escrito da Hyland.

d. O Cliente poderá realizar testes de penetração no URL público usado para acessar o Serviço de Nuvem da Hyland anualmente; contanto que o Cliente avise a Hyland por escrito de seu desejo de realizar esses testes e os seguintes critérios sejam atendidos: (a) a Hyland e o Cliente concordem mutuamente com o tempo, o escopo e os critérios de tais testes, que podem incluir técnicas comuns de engenharia social, aplicação e teste de rede usadas para identificar ou explorar vulnerabilidades comuns, incluindo transbordamento da memória, scripts entre sites, injeção de SQL, e ataques man-in-the-middle, e (b) esse teste seja feito aos custos e despesas do Cliente e que o Cliente pague as taxas da Hyland (às taxas padrão da Hyland) pelos Serviços Profissionais que são exigidos ou solicitados da Hyland em conexão com esses testes. Antes de qualquer teste, qualquer terceiro contratado pelo Cliente para auxiliá-lo deve ser instruído pela Hyland e assinar um Contrato de Não Divulgação diretamente com a Hyland. O Cliente reconhece e concorda que qualquer teste realizado sem acordo mútuo em relação a tempo, escopo e critérios pode ser considerado um ataque hostil, o que pode desencadear respostas automáticas e manuais, incluindo o relato da atividade a órgãos regulatórios locais e federais, bem como a suspensão imediata do acesso ou uso pelo Cliente do Serviço de Nuvem da Hyland. É proibido ao Cliente distribuir ou publicar os resultados de tais testes de penetração a terceiros sem a aprovação prévia por escrito da Hyland.