A tradução abaixo é oferecida apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês (principalmente devido a atrasos na tradução), a versão em inglês prevalecerá.

POLÍTICA DE SEGURANÇA PARA FORNECEDORES

Última atualização em 28 de janeiro de 2022

1. ESCOPO; DEFINIÇÕES.

1.1 Política de segurança. O Fornecedor cumprirá, em todos os aspectos, as exigências de segurança da informação da Amazon estabelecidas nesta política ("**Política de segurança**"). Esta Política de segurança aplica-se ao desempenho do Fornecedor nos termos do Contrato e a todo acesso, coleta, uso, armazenamento, transmissão, divulgação, destruição ou exclusão das Informações da Amazon pelo Fornecedor, bem como a incidentes de segurança relacionados às Informações da Amazon. Esta Política de segurança não limita nenhuma outra obrigação do Fornecedor, inclusive nos termos de outros contratos com a Amazon ou outras leis que se apliquem ao Fornecedor, ao desempenho do Fornecedor nos termos de outros contratos com a Amazon, às Informações da Amazon ou à Finalidade permitida. Se esta Política de segurança entrar em conflito com algum contrato de confidencialidade entre as partes ou com outros contratos aplicáveis às partes, o Fornecedor notificará imediatamente a Amazon sobre o conflito e cumprirá as exigências que sejam mais protetoras das Informações da Amazon, salvo se as exigências menos protetoras sejam expressamente declaradas como anulando as exigências mais protetoras (o que poderá ser designado pela Amazon). A Amazon poderá alterar esta Política de segurança ao longo do tempo, a seu exclusivo critério, contanto que, se estas alterações não forem comercialmente possíveis, mediante solicitação, a Amazon cumprirá e definirá, de comum acordo, taxas adicionais adequadas.

1.2 Definições.

1.2.1 "**Agregar**" refere-se a combinar ou armazenar Informações da Amazon com dados ou informações do Fornecedor ou de terceiros.

1.2.2 "**Contrato**" refere-se a qualquer contrato que faça referência a esta Política de segurança.

1.2.3 "**Amazon**" refere-se à Amazon.com, Inc. e suas respectivas afiliadas.

1.2.4 "**Anonimizar**" refere-se a usar, coletar, armazenar, transmitir ou transformar dados ou informações (inclusive Informações da Amazon) de maneira ou forma que não identifique, permita a identificação e não seja, de outra forma, atribuível à Amazon ou a qualquer usuário, identificador de dispositivo, fonte, produto, serviço, contexto ou marca da Amazon.

1.2.5 "**Informações da Amazon**" refere-se, individual e coletivamente, a: (a) todas as Informações confidenciais da Amazon (conforme definido no contrato de confidencialidade ou outro contrato entre as partes); (b) todos os outros dados, registros, arquivos, conteúdo ou informações, em qualquer forma ou formato, adquiridas, acessadas, coletadas, recebidas, armazenadas ou mantidas pelo Fornecedor ou por suas respectivas afiliadas, da Amazon ou em nome dela ou, de outra forma, relacionadas a esta Política de segurança ou aos serviços, ou ao desempenho ou exercício dos direitos das partes relacionados ou nos termos do Contrato; e (c) informações derivadas de (a) ou (b), mesmo se Anonimizadas.

1.2.6 "Fornecedor" refere-se a cada Fornecedor, Prestador de serviços ou Contratado definido no Contrato e qualquer outro prestador de serviços sujeito a um Contrato.

1.3 Finalidade permitida. O Fornecedor poderá acessar, coletar, usar, armazenar e transmitir apenas as Informações da Amazon expressamente autorizadas nos termos do Contrato e exclusivamente com a finalidade de fornecer os produtos ou serviços nos termos do Contrato, de acordo com as licenças (se houver) concedidas nos termos desta Política de segurança ("**Finalidade permitida**"). Salvo conforme expressamente autorizado

nos termos do Contrato, o Fornecedor não acessará, coletará, usará, armazenará ou transmitirá Informações da Amazon nem agregará Informações da Amazon, mesmo que Anonimizadas. Salvo mediante o consentimento prévio e expresso por escrito da Amazon, o Fornecedor não (a) transferirá, alugará, permutará, comercializará, venderá, emprestará ou arrendará ou, de outra forma, distribuirá ou disponibilizará a qualquer terceiro as Informações da Amazon nem (b) Agregará Informações da Amazon com outras informações ou dados, mesmo que Anonimizados.

2. POLÍTICA DE SEGURANÇA DA AMAZON.

2.1 Exigências básicas de segurança. O fornecedor, de maneira consistente com os padrões recomendados atuais do setor e com outras exigências especificadas pela Amazon com base na classificação e sensibilidade das Informações da Amazon, manterá as proteções físicas, administrativas e técnicas, bem como outras medidas de segurança para (a) manter a segurança e a confidencialidade das Informações da Amazon acessadas, coletadas, usadas, armazenados ou transmitidas pelo Fornecedor, e (b) protegerá essas informações contra ameaças ou perigos conhecidos ou razoavelmente previstos à segurança e integridade, perda acidental, alteração e divulgação das Informações da Amazon, bem como de todas as outras formas ilegais de processamento. Entre outras, o Fornecedor cumprirá as seguintes exigências no que diz respeito a todos os sistemas que o Fornecedor usar para processar as Informações da Amazon ou que tenham acesso às Informações da Amazon ("**Sistemas de Informação da Amazon**"):

2.1.1 Segurança de rede. O Fornecedor protegerá os Sistemas de Informação da Amazon restringindo o acesso não autorizado à rede, especialmente da internet externa. O Fornecedor instalará e manterá uma solução de segurança de rede eficaz, como um firewall, para proteger as Informações da Amazon em todos os momentos.

2.1.2 Atualizações. Conforme descrito na Publicação Especial (Special Publication, "SP") 800-40, Revisão 3, do Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, "NIST") (NIST SP 800-40), o Fornecedor manterá os Sistemas de Informação da Amazon atualizados com as mais recentes melhorias, atualizações, correções de bugs e novas versões e com outras modificações necessárias para assegurar a segurança das Informações da Amazon.

2.1.3 Antimalware. O Fornecedor sempre usará software antimalware ou controle de segurança equivalente para mitigar o risco de comprometimento e disseminação de malware. Se usado, o Fornecedor manterá o software antimalware atualizado.

2.1.4 Criptografia. O Fornecedor criptografará os dados em repouso e os dados enviados por meio de redes abertas de acordo com as práticas recomendadas do setor.

2.1.5 Testes. O Fornecedor testará regularmente seus respectivos sistemas e processos de segurança para assegurar que atendam às exigências desta Política de segurança ou à política de segurança acordada pela última vez pelo Fornecedor e pela Amazon. Havendo alterações na Política de segurança nos termos da Seção 1.1, as alterações não entrarão em vigor para os fins desta Seção antes do acordo entre o Fornecedor e a Amazon (e-mail é suficiente).

2.1.6 Controles de acesso. O Fornecedor protegerá as Informações da Amazon, inclusive cumprindo as seguintes exigências:

2.1.6.1 O Fornecedor atribuirá uma ID exclusiva a cada pessoa com acesso de computador às Informações da Amazon ou aos Sistemas de Informação da Amazon.

2.1.6.2 O Fornecedor restringirá o acesso às Informações da Amazon apenas às pessoas com "necessidade de saber" para a Finalidade permitida.

2.1.6.3 O Fornecedor revisará regularmente a lista de pessoas e serviços com acesso às Informações da Amazon e removerá contas que não precisem mais de acesso aos Sistemas de Informação da Amazon. Essa revisão precisa ser realizada, no mínimo, uma vez a cada 90 dias.

2.1.6.4 O Fornecedor não usará padrões fornecidos pelo fabricante para senhas do sistema e outros parâmetros de segurança em nenhum Sistema de Informação da Amazon. O Fornecedor obrigará e assegurará o uso de "senhas fortes" impostas pelo sistema de acordo com as práticas

recomendadas descritas na NIST SP 800-63B em todos os Sistemas de Informação da Amazon. O Fornecedor exigirá que todas as senhas e credenciais de acesso sejam mantidas confidenciais e não compartilhadas entre os funcionários.

2.1.6.5 O Fornecedor manterá e aplicará o "bloqueio de conta", desativando contas com acesso às Informações da Amazon ou aos Sistemas de Informação da Amazon quando a conta exceder mais de 10 (dez) tentativas de senha incorreta consecutivas.

2.1.6.6 Salvo se expressamente autorizado pela Amazon por escrito, o Fornecedor segregará física ou logicamente as Informações da Amazon em todos os momentos (inclusive em armazenamento, processamento ou transmissão) das informações do Fornecedor e de terceiros.

2.1.6.7 Se controles de acesso físico adicionais forem solicitados por escrito pela Amazon, o Fornecedor implementará e usará essas medidas de controle de acesso físico seguro.

2.1.6.8 Mediante solicitação da Amazon, o Fornecedor fornecerá à Amazon (a) dados de registro sobre todo o uso (autorizado e não autorizado) das contas ou credenciais da Amazon fornecidas ao Fornecedor para a Finalidade permitida (p. ex., credenciais de conta social) e (b) dados de registro detalhados sobre personificação ou tentativa de personificar os funcionários da Amazon ou do Fornecedor que tenham acesso às Informações da Amazon.

2.1.6.9 O Fornecedor revisará regularmente os registros de acesso com relação a sinais de comportamento malicioso ou acesso não autorizado.

2.1.7 Política do fornecedor. O Fornecedor manterá e aplicará uma política de segurança das informações e rede para funcionários, subcontratados, agentes e fornecedores que atenda às normas estabelecidas nesta Política de segurança, inclusive métodos para detecção e registro de violações da política. Mediante solicitação da Amazon, o Fornecedor fornecerá à Amazon informações sobre violações das informações e da política de segurança de rede do Fornecedor se o Fornecedor ou a Amazon tiver alguma suspeita de que isso possa constituir um Incidente de segurança (conforme definição abaixo).

2.1.8 Subcontratos. O Fornecedor não subcontratará ou delegará nenhuma das suas respectivas obrigações nos termos desta Política de segurança a nenhum subcontratado ou representante (em conjunto, "**Subcontratados**") sem o consentimento prévio por escrito da Amazon. Não obstante a existência ou os termos do subcontrato ou delegação, o Fornecedor permanecerá responsável pelo pleno cumprimento das suas respectivas obrigações nos termos desta Política de segurança. Os termos e condições desta Política de segurança serão vinculativos para os Subcontratados e funcionários do Fornecedor. O Fornecedor (a) assegurará que seus respectivos Subcontratados e funcionários cumpram esta Política de segurança e (b) será responsável por todos os atos, omissões, negligência e má conduta dos Subcontratados e funcionários do Fornecedor

2.1.9 Acesso remoto. O Fornecedor assegurará que o acesso aos Sistemas de Informação da Amazon exija autenticação multifatorial (p. ex., que requeira, no mínimo, dois fatores separados para identificar usuários).

2.1.10 Acesso "em massa". Para os fins desta seção, acesso "em massa" refere-se a acessar dados por meio de consulta de banco de dados, geração de relatórios ou outra transferência de dados em massa. Salvo se expressamente autorizado por escrito pela Amazon, o Fornecedor não acessará e não permitirá o acesso "em massa" às Informações da Amazon, independentemente das Informações da Amazon estarem em um banco de dados controlado pelo Fornecedor ou pela Amazon ou armazenadas de outra maneira, inclusive armazenamento em arquivos baseados em arquivos (p. ex., arquivos simples), etc. Especificamente, esta seção proíbe o acesso às Informações da Amazon, salvo o acesso a registros individuais, conforme necessário para a Finalidade permitida. O Fornecedor preservará os dados de registro detalhados sobre a tentativa ou realização do acesso "em massa" às Informações da Amazon e fornecerá relatórios desses registros como parte das obrigações do Fornecedor nos termos da Seção 2.5 (Revisão de segurança). Se a Amazon fornecer ao Fornecedor autorização por escrito para o acesso "em massa" às Informações da Amazon, o Fornecedor (a) limitará esse acesso apenas a funcionários especificados com uma "necessidade de saber" e (b) usará ferramentas que limitem o acesso e exijam autorização explícita e registro de todos os acessos.

2.1.11 Funcionários do fornecedor. A Amazon poderá condicionar o acesso dos funcionários do Fornecedor às Informações da Amazon à sua respectiva execução e entrega à Amazon de contratos de confidencialidade individuais, cuja forma é especificada pela Amazon. Os funcionários do Fornecedor assinarão o contrato de confidencialidade individual, se a Amazon assim exigir. O Fornecedor obterá e entregará à Amazon contratos de confidencialidade individuais assinados pelos funcionários do Fornecedor que terão acesso às Informações da Amazon (antes de conceder acesso ou fornecer informações aos funcionários do Fornecedor). O Fornecedor também manterá uma lista de todos os funcionários do Fornecedor que acessaram ou receberam as Informações da Amazon nos Sistemas de Informação da Amazon e fornecerá essa lista imediatamente à Amazon, mediante solicitação. Com relação aos funcionários do Fornecedor que (a) não precisem mais de acesso às Informações da Amazon ou (b) não se qualifiquem mais como funcionários do Fornecedor (p. ex., a pessoa deixa de ser funcionário do Fornecedor), o Fornecedor cancelará imediatamente (no prazo máximo de 24 horas) o acesso às Informações da Amazon e aos Sistemas de Informação da Amazon. Se algum desses funcionários estiver autorizado a acessar as Informações da Amazon nos Sistemas de Informação da Amazon, o Fornecedor também notificará a Amazon no prazo de 24 horas.

2.2 Acesso aos portais da Extranet da Amazon e do Fornecedor. A Amazon poderá conceder ao Fornecedor acesso às Informações da Amazon por meio de portais da internet ou outros sites não públicos ou serviços de extranet no site ou sistema da Amazon ou de terceiros (cada, uma "**Extranet**") para a Finalidade permitida. Se a Amazon permitir que o Fornecedor acesse Informações da Amazon usando uma Extranet, o Fornecedor precisará cumprir as seguintes exigências:

2.2.1 Finalidade permitida. O Fornecedor e os funcionários do Fornecedor acessarão a Extranet e acessarão, coletarão, usarão, visualizarão, recuperarão, baixarão ou armazenarão Informações da Amazon por meio da Extranet exclusivamente para a Finalidade permitida.

2.2.2 Contas. O Fornecedor assegurará que os funcionários do Fornecedor usem apenas as contas da Extranet designadas pela Amazon para cada indivíduo e exigirá que os funcionários do Fornecedor mantenham suas respectivas credenciais de acesso confidenciais.

2.2.3 Sistemas. O Fornecedor acessará a Extranet apenas por meio de aplicativos ou sistemas de computação ou processamento que executem sistemas operacionais gerenciados pelo Fornecedor e que incluam: (a) firewalls de rede do sistema de acordo com a Seção 2.1.1 (Segurança de rede); (b) gestão centralizada de patches em conformidade com a Seção 2.1.2 (Atualizações); (c) software antimalware adequado para o sistema operacional de acordo com a Seção 2.1.3 (Antimalware); e (d) criptografia de disco completa para dispositivos portáteis.

2.2.4 Restrições. Salvo se aprovado antecipadamente por escrito pela Amazon, o Fornecedor não baixará, espelhará ou armazenará permanentemente Informações da Amazon por meio de qualquer Extranet em nenhum meio, inclusive máquinas, dispositivos ou servidores.

2.2.5 Encerramento da conta. O Fornecedor encerrará a conta e notificará a Amazon em até 24 horas após o funcionário do Fornecedor autorizado a acessar a Extranet: (a) não precisar mais acessar as Informações da Amazon ou (b) não se qualificar mais como funcionário do Fornecedor (p. ex., deixar de ser funcionário do Fornecedor).

2.2.6 Sistemas de terceiros.

2.2.6.1 O Fornecedor notificará a Amazon com antecedência e obterá a aprovação prévia por escrito da Amazon antes de usar qualquer sistema de terceiros que armazene ou possa ter acesso às Informações da Amazon, salvo se (a) os dados forem criptografados de acordo com esta Política de segurança e (b) o sistema de terceiros não tiver acesso à chave de descriptografia ou às versões de "texto simples" não criptografadas dos dados. A Amazon reserva-se o direito de exigir uma revisão de segurança da Amazon [de acordo com a Seção 2.5 (Revisão de segurança)] do sistema de terceiros antes de conceder a aprovação.

2.2.6.2 Se o Fornecedor usar sistemas de terceiros que armazenem Informações da Amazon não criptografadas ou que, de outra forma, possam acessar Informações da Amazon não criptografadas, o Fornecedor realizará uma revisão de segurança dos sistemas de terceiros e dos seus respectivos controles de segurança e fornecerá à Amazon relatórios periódicos sobre os controles de segurança

do sistema de terceiros no formato solicitado pela Amazon (p. ex., SAS 70 ou relatório sucessor, ou outro relatório padrão do setor reconhecido aprovado pela Amazon).

2.3 Preservação e destruição de dados.

2.3.1 Preservação. O Fornecedor preservará as Informações da Amazon apenas para a finalidade e pelo tempo necessário para a Finalidade permitida.

2.3.2 Devolução ou exclusão. Mediante solicitação da Amazon, o Fornecedor devolverá imediatamente (mas, no máximo, em 72 horas) à Amazon e excluirá de forma permanente e segura todas as Informações da Amazon de acordo com a notificação da Amazon que exija a devolução e/ou exclusão. O Fornecedor também excluirá de forma permanente e segura todas as instâncias ao vivo (on-line ou acessíveis por rede) das Informações da Amazon no prazo de 30 dias após a conclusão da Finalidade permitida ou rescisão ou expiração desta Política de segurança, o que ocorrer primeiro. Se solicitado pela Amazon, o Fornecedor certificará por escrito que todas as Informações da Amazon foram destruídas. A título de esclarecimento, esta seção não se aplicará às Cópias de arquivamento de acordo com a Seção 2.3.3

2.3.3 Cópias de arquivamento. Se o Fornecedor for obrigado por lei a preservar cópias de arquivamento das Informações da Amazon para fins fiscais ou regulatórios semelhantes, as Informações da Amazon arquivadas precisam ser armazenadas de uma das seguintes maneiras:

2.3.3.1 Como backup "frio" ou off-line (ou seja, não disponível para uso imediato ou interativo) armazenado em uma instalação fisicamente segura.

2.3.3.2 Criptografadas, no qual o sistema que hospeda ou armazena os arquivos criptografados não tem acesso à cópia das chaves usadas para criptografia.

2.3.4 Recuperação. Se o Fornecedor realizar uma "recuperação" (ou seja, reverter para backup) para fins de recuperação de desastres, o Fornecedor terá e manterá um processo que assegure que todas as Informações da Amazon que precisem ser excluídas de acordo com o Contrato, com esta Política de segurança ou outro contrato com a Amazon sejam excluídas ou substituídas dos dados recuperados de acordo com esta Seção 2.3 no prazo de 24 horas a contar do momento da recuperação. Se o Fornecedor realizar uma recuperação para qualquer finalidade, nenhuma Informação da Amazon poderá ser recuperada para qualquer sistema ou rede de terceiros sem a aprovação prévia por escrito da Amazon. A Amazon reserva-se o direito de exigir uma revisão de segurança da Amazon [de acordo com a Seção 2.5 (Revisão de segurança)] do sistema ou da rede de terceiros antes de permitir a recuperação das Informações da Amazon para sistemas ou redes de terceiros.

2.3.5 Padrões de sanitização de dados. Todas as Informações da Amazon excluídas pelo Fornecedor serão excluídas de acordo com as Recomendações mínimas de sanitização contidas na NIST SP 800-88, Revisão 1, Diretrizes para sanitização de mídia, 18 de dezembro de 2014 (disponível em http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Anexo A, para purgar o tipo de dispositivo relevante. Na ausência de orientações relevantes na NIST SP 800-88, Anexo A, o dispositivo contendo Informações da Amazon será destruído de uma das seguintes maneiras: (a) por meio da desmagnetização de mídia magnética em um campo de fluxo eletromagnético de mais de 10.000 Gauss; (b) por trituração ou desintegração mecânica que resulte em partículas menores que 2x2 mm; ou (c) por meio de outros padrões que a Amazon possa exigir com base na classificação e na sensibilidade das informações da Amazon.

2.4 Destruição forense. Antes de descartar (de qualquer forma) qualquer hardware, software ou outra mídia que tenha ou contenha, a qualquer momento, Informações da Amazon, o Fornecedor realizará uma destruição forense completa do hardware ou software, ou de outra mídia, de forma que a recuperação das Informações da Amazon em qualquer forma seja inviável. O Fornecedor realizará a destruição forense de acordo com as Recomendações mínimas de sanitização contidas na NIST SP 800-88, Anexo A, para destruir o tipo de dispositivo em questão.

2.4.1 O Fornecedor não venderá, revenderá, doará, recondicionará ou, de outra forma, transferirá (inclusive qualquer venda ou transferência de hardware, software ou outra mídia, qualquer disposição relacionada a liquidação dos negócios do Fornecedor ou qualquer outra disposição) qualquer hardware, software ou outra mídia que contenha Informações da Amazon que não tenha sido forensicamente destruída pelo Fornecedor, conforme exigido por esta Seção 2.4.

2.5 Revisão de segurança.

2.5.1 A Amazon reserva-se o direito de solicitar periodicamente ao Fornecedor que participe de uma avaliação de riscos da Amazon.

2.5.2 Certificação. Mediante solicitação por escrito da Amazon, o Fornecedor certificará por escrito à Amazon que as informações fornecidas como parte da avaliação de riscos estão em conformidade com esta Política de segurança acordada pela última vez pelo Fornecedor e pela Amazon. Havendo alterações na Política de segurança nos termos da Seção 1.1, as alterações não entrarão em vigor para os fins desta Seção antes do acordo entre o Fornecedor e a Amazon (e-mail é suficiente).

2.5.3 Outras revisões. A Amazon reserva-se o direito de revisar periodicamente a segurança dos Sistemas de Informação da Amazon, mas, no máximo, uma vez por ano, salvo se (a) uma deficiência substancial anterior tenha sido identificada durante o ano ou (b) a Amazon seja obrigada por uma agência governamental ou outro órgão regulatório a realizar esta revisão. O Fornecedor cooperará e fornecerá à Amazon todas as informações necessárias dentro de um prazo razoável, mas, no máximo, 20 dias corridos a partir da data da solicitação da Amazon.

2.5.4 Correção. Se alguma revisão de segurança identificar deficiências, o Fornecedor, às custas e despesas exclusivas do Fornecedor, tomará todas as medidas possíveis necessárias para corrigir as deficiências dentro de um prazo definido.

2.6 Incidentes de segurança.

2.6.1 O Fornecedor informará a Amazon o mais rápido possível, mas, no máximo, 24 horas após o Fornecedor tomar conhecimento de acesso não autorizado, coleta, aquisição, uso, transmissão, divulgação, corrupção ou perda, real ou suspeita, das Informações da Amazon ou violação dos Sistemas de Informação da Amazon ("**Incidente de segurança**"). O Fornecedor solucionará cada Incidente de segurança em tempo hábil e fornecerá à Amazon detalhes por escrito sobre a investigação interna do Fornecedor em relação a cada Incidente de segurança. Quando permitido pela legislação aplicável, o Fornecedor concorda em não notificar nenhuma autoridade reguladora ou cliente em nome da Amazon, salvo se a Amazon solicitar especificamente por escrito que o Fornecedor o faça, e a Amazon reserva-se o direito de revisar e aprovar a forma e o conteúdo de qualquer notificação antes que seja fornecida a qualquer parte. O Fornecedor cooperará e trabalhará em conjunto com a Amazon para formular e executar um plano para retificar todos os Incidentes de segurança confirmados.

2.6.2 Na medida permitida pela legislação aplicável, caso o Fornecedor receba um pedido ou determinação de algum órgão administrativo (como intimação, ordem judicial ou mandado de busca) buscando dados que incluam Informações da Amazon, o Fornecedor notificará a Amazon em tempo hábil para permitir que a Amazon busque uma ordem de proteção ou outro recurso cabível.

2.7 Disposições gerais. A Amazon detém o critério exclusivo de tomar todas as decisões aplicáveis nos termos desta Política de segurança. Qualquer lista de exemplos após "inclusive" ou "p. ex." é ilustrativa e não completa. Todas as referências às normas de exigências de segurança nos termos desta Política de segurança referem-se às normas especificadas e suas respectivas versões sucessoras ou equivalentes, conforma possam ser atualizadas, salvo se a Amazon especificar de outra forma.