A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

POLÍTICA DE SEGURANÇA PARA FORNECEDORES DA AMAZON

Última atualização: 11 de setembro de 2024

1. **ESCOPO**. O Fornecedor cumprirá estas exigências de segurança ("Política de segurança"). Esta Política de segurança não limita nenhuma outra obrigação contratual ou jurídica do Fornecedor. Na medida em que houver algum conflito entre esta Política de segurança e outros contratos entre o Fornecedor e a Amazon, o Fornecedor cumprirá as exigências mais restritivas que melhor protejam as Informações da Amazon.

2. **ATUALIZAÇÕES**.

2.1 A Amazon poderá fazer atualizações comercialmente justificáveis a esta Política de segurança ao longo do tempo, que entrarão em vigor 30 dias após a data da "Última atualização" desta Política de segurança. O Fornecedor concorda em vincular-se à Política de segurança atualizada assim que as atualizações entrarem em vigor.

2.2 Se desejar receber aviso prévio das atualizações antes de entrarem em vigor, o Fornecedor poderá se inscrever para receber notificações de atualização usando o formulário de assinatura fornecido na página da Política de segurança. O Fornecedor assegurará que todas as informações de contato do Fornecedor registradas para o recebimento das notificações de atualização estejam sempre atualizadas e precisas. Será considerado que o Fornecedor recebeu a notificação de atualização relevante quando esta for enviada por e-mail, independentemente de o Fornecedor efetivamente receber ou não a notificação de atualização.

3. **FINALIDADE PERMITIDA**.

3.1 **Autorização expressa**. O Fornecedor poderá Processar 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 ("Finalidade permitida").

3.2 **Preservação de dados**. O Fornecedor preservará as Informações da Amazon exclusivamente para a finalidade e pelo tempo necessário para a Finalidade permitida.

3.3 **Limitações expressas**. O Fornecedor: (a) não Processará nenhuma Informação da Amazon, mesmo que Anonimizada; (b) não transferirá, alugará, permutará, negociará, venderá, emprestará, arrendará ou, de outra forma, distribuirá ou disponibilizará a terceiros qualquer Informação da Amazon, mesmo que Anonimizada; ou, (c) não desenvolverá, treinará ou aprimorará qualquer modelo de Inteligência artificial (IA) ou Aprendizado de máquina (*Machine Learning*, ML) usando as Informações da Amazon, mesmo que Anonimizadas.

4. **EXIGÊNCIAS MÍNIMAS DE SEGURANÇA**. O Fornecedor manterá proteções físicas, administrativas e técnicas consistentes com as práticas recomendadas do setor [inclusive com as normas 27001 e 27002 da Organização Internacional de Normalização (*International Organization for Standardization*, "ISO"), com a Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology*, "NIST") ou com outras
normas semelhantes]. As proteções mantidas pelo Fornecedor incluirão as exigências mínimas descritas abaixo nas Subcláusulas 4.1 a 4.18.

4.1 **Programa de segurança da informação por escrito**. O Fornecedor terá um programa de segurança da informação por escrito que: (a) inclua políticas, procedimentos e normas adequados que atendam às exigências estabelecidas nesta Política de segurança; (b) atribua um ponto de contato de segurança responsável por comunicar e gerenciar questões de segurança (inclusive Incidentes de segurança); (c) seja revisado, no mínimo, anualmente e atualizado conforme necessário; e, (d) seja aplicável aos Funcionários. O Fornecedor monitorará e aplicará o programa de segurança da informação e abordará qualquer violação.

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

4.2 **Gerenciamento de patches**. O Fornecedor manterá atualizados os Sistemas de informação cobertos, com as atualizações mais recentes, correções de erros e novas versões. O Fornecedor implementará mitigações para ativos não passíveis de aplicação de patches.

4.3 **Registro**. O Fornecedor coletará, gerenciará e preservará registros de auditoria, eventos e segurança, inclusive: (a) dados de registro sobre todo o uso (autorizado e não autorizado) das contas ou credenciais da Amazon fornecidas ao Fornecedor para uma Finalidade permitida; e, (b) dados de registro sobre qualquer personificação ou tentativa de personificar qualquer funcionário da Amazon ou os Funcionários com acesso às Informações da Amazon ou aos Sistemas de informação cobertos. Em relação a cada evento registrado, estes registros conterão dados suficientes para identificar: (i) os Funcionários ou a conta que iniciou o evento; (ii) o horário do evento; e, (iii) o sistema, dados ou outros recursos afetados. O Fornecedor analisará regularmente estes registros para ajudar a detectar, investigar e fazer a recuperação das atividades não autorizadas.

4.4 **Defesas contra malware**. O Fornecedor: (a) implantará software antimalware ou um controle de segurança equivalente para todos os Sistemas de informação cobertos; (b) manterá as atualizações, assinaturas e configurações do software antimalware ou controle de segurança equivalente; e, (c) configurará sistemas para detectar, prevenir e corrigir a instalação, disseminação e execução de código malicioso ou não autorizado.

4.5 **Programa de gestão de riscos**. O Fornecedor terá um programa de gestão de riscos de segurança da informação por escrito, que define processos para análise de risco, tratamento de risco, aceitação de risco e exceções.

4.6 **Treinamento de conscientização sobre segurança**. O Fornecedor proporcionará treinamento sobre segurança da informação e privacidade de dados aos Funcionários na contratação e, no mínimo, anualmente a partir de então. O Fornecedor também assegurará que os Funcionários sejam informados em tempo hábil sobre as atualizações das políticas de segurança e privacidade de dados do Fornecedor.

4.7 **Inventário de dados**. O Fornecedor documentará e manterá informações sobre: (a) quais Informações da Amazon estão sendo Processadas; e, (b) como e onde estas Informações da Amazon são Processadas (p. ex., em um diagrama de arquitetura atualizado). Mediante solicitação da Amazon, o Fornecedor disponibilizará estas informações à Amazon.

4.8 **Testes de segurança**.

4.8.1 O Fornecedor realizará testes anuais para assegurar que está em conformidade com as exigências desta Política de segurança.

4.8.2 O Fornecedor realizará testes de penetração das defesas de segurança do Fornecedor, no mínimo, anualmente. Os testes de penetração incluirão: (a) testes dentro e fora da rede do Fornecedor; (b) engenharia social (p. ex., simulações de phishing); e, (c) testes de segurança para redes sem fio. O Fornecedor abordará as vulnerabilidades identificadas como parte do programa de gestão de vulnerabilidades. Mediante solicitação da Amazon, o Fornecedor disponibilizará à Amazon os resultados destes testes de penetração e correção de vulnerabilidades.

4.9 **Segurança de rede**. O Fornecedor protegerá os Sistemas de informação cobertos restringindo o acesso não autorizado à rede, especialmente de redes externas. O Fornecedor manterá e configurará firewalls ou outros controles de segurança equivalentes para proteger os sistemas contra acesso não autorizado e revisará os conjuntos de regras de firewall, no mínimo, anualmente para assegurar que casos de negócios válidos e documentados existam para todas as regras.

4.10 **Ambiente adequado**. O Fornecedor Processará as Informações da Amazon apenas em ambientes adequados à sua respectiva finalidade e não Processará as Informações da Amazon em ambientes de teste, salvo se permitido pelo Contrato.

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

4.11 **Criptografia**. O Fornecedor criptografará todas as Informações da Amazon em repouso e em trânsito por meio de redes externas, de acordo com as práticas recomendadas do setor. Se as Informações da Amazon forem transmitidas em redes internas do Fornecedor, estas informações serão transmitidas por meio de um protocolo criptografado que atenda às práticas recomendadas do setor. O Fornecedor gerenciará e protegerá as chaves de criptografia de acordo com as práticas recomendadas do setor.

4.12 **Uso controlado de privilégios administrativos**. O Fornecedor gerenciará as funções administrativas de acordo com a Estrutura de segurança cibernética do NIST ou da ISO 27002. O Fornecedor separará, no mínimo, as contas administrativas das contas padrão e restringirá as contas administrativas aos recursos necessários para realizar as funções administrativas. O Fornecedor registrará todas as ações administrativas da conta de maneira atribuível a um usuário individual. Os recursos administrativos disponibilizados para uma conta padrão terão privilégios mínimos e serão registrados de maneira atribuível a um usuário individual.

4.13 **Controle de acesso**.

4.13.1 **IDs exclusivas**. O Fornecedor atribuirá IDs individuais e exclusivas aos Funcionários com acesso às Informações da Amazon ou aos Sistemas de informação cobertos, inclusive contas com acesso administrativo.

4.13.2 **Base exclusiva na "necessidade de saber"**. O Fornecedor restringirá o acesso às Informações da Amazon e aos Sistemas de informação cobertos exclusivamente aos Funcionários com "necessidade de saber" para a Finalidade permitida.

4.13.3 **Revisão de acesso do usuário**. O Fornecedor revisará, no mínimo uma vez a cada 90 dias, a lista de Funcionários e serviços com acesso às Informações da Amazon e aos Sistemas de informação cobertos e removerá contas que não precisem mais de acesso.

4.13.4 **Autenticação única (SSO**). Qualquer serviço do Fornecedor que exija autenticação de funcionários da Amazon precisa se integrar a um provedor de identidade da Amazon (p. ex., Amazon Federate) para fornecer essa autenticação. Estes serviços não poderão usar credenciais fornecidas pelo Fornecedor ou gerenciadas pelo Fornecedor para autenticação.

4.14 **Gestão de senhas**.

4.14.1 **Senhas fortes**. O Fornecedor não usará padrões fornecidos pelo fabricante para senhas do sistema e outros parâmetros de segurança em nenhum Sistema de informação coberto. O Fornecedor obrigará e assegurará o uso de "senhas fortes" impostas pelo sistema, de acordo com as práticas recomendadas descritas no NIST SP 800-63B, em todos os Sistemas de informação cobertos. O Fornecedor exigirá que todas as senhas e credenciais de acesso sejam mantidas em confidencialidade e que não sejam compartilhadas entre os Funcionários.

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

4.15 **Acesso remoto; Autenticação multifator**. O Fornecedor implementará autenticação multifator (ou seja, exigência de, no mínimo, dois fatores para autenticar o usuário) para acesso remoto a qualquer rede, sistema, aplicativo ou outro ativo do Fornecedor.

4.16 **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.

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

4.16.1 Salvo se expressamente estabelecido no Contrato ou, de outra forma, por escrito pela Amazon, o Fornecedor não acessará e não permitirá o acesso “em massa” às Informações da Amazon, independentemente de as Informações da Amazon estarem em um banco de dados controlado pelo Fornecedor ou pela Amazon ou armazenadas de qualquer outra maneira, inclusive armazenamento em arquivos baseados em arquivos (p. ex., arquivos simples).

4.16.2 Se a Amazon autorizar acesso “em massa”, o Fornecedor: (a) limitará esse acesso aos Funcionários especificados com uma “necessidade de saber”; e, (b) exigirá autorização explícita e registro deste acesso de acordo com as exigências da Subcláusula 4.3. Mediante solicitação da Amazon, em coordenação com as revisões de segurança da Cláusula 10 ou com os Incidentes de segurança da Cláusula 11, o Fornecedor disponibilizará à Amazon todos os registros sobre o acesso “em massa” referenciado nesta seção.

4.17 Segregação de dados. O Fornecedor sempre separará física ou logicamente as Informações da Amazon das informações do Fornecedor e de terceiros. Se a segregação não for possível, o Fornecedor assegurará que as Informações da Amazon sejam distinguíveis de outras informações para fins de registro, exclusão e resposta a incidentes.

4.18 **Segurança dos Funcionários do Fornecedor**.

4.18.1 O Fornecedor tomará todas as precauções cabíveis para assegurar que os Funcionários que tenham acesso às Informações da Amazon mantenham a confidencialidade das informações e as usem exclusivamente para a Finalidade permitida. Estas precauções precisam incluir a imposição de exigências de confidencialidade por meio de um contrato de confidencialidade ou política do Fornecedor.

4.18.2 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, o Fornecedor cancelará, em até 24 horas, o acesso às Informações da Amazon e aos Sistemas de informação cobertos. Se qualquer Funcionário mantiver acesso às Informações da Amazon ou aos Sistemas de informação cobertos por mais de 24 horas após (a) ou (b) ocorrer, o Fornecedor notificará a Amazon sobre este acesso contínuo em até 24 horas após o Fornecedor tomar conhecimento deste acesso, enviando um e-mail para security@amazon.com.

5. **EXIGÊNCIAS DE SEGURANÇA PARA PAGAMENTOS**. Se o Fornecedor tiver acesso ou Processar dados de titulares de cartões de pagamento, o Fornecedor estará em conformidade com a versão mais recente do Padrão de segurança de dados da Indústria de cartões de pagamento (*Payment Card Industry Data Security Standard*, PCI DSS).

6. **SUBCONTRATADOS**.

6.1 O Fornecedor não subcontratará nem delegará nenhuma das suas respectivas obrigações nos termos desta Política de segurança a terceiros (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.

6.2 Se o Fornecedor usar qualquer Sistema de informação coberto do Subcontratado, o Fornecedor realizará uma análise de segurança do Sistema de informação coberto do Subcontratado e dos respectivos controles de segurança e, mediante solicitação da Amazon, enviará à Amazon relatórios periódicos sobre os controles de segurança do Sistema de informação coberto do Subcontratado, no formato solicitado pela Amazon [p. ex., Declaração sobre as normas para compromissos de certificação n.º 16 (*Statement on Standards for Attestation Engagements*, SSAE 16)].

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

7. ACESSO AOS SISTEMAS DE INFORMAÇÃO GERENCIADOS PELA AMAZON. A Amazon poderá conceder ao Fornecedor o direito de Processar as Informações da Amazon por meio de portais da internet ou outros sites ou extranets privadas (cada, um "Sistema de informação gerenciado pela Amazon"), exclusivamente para a Finalidade permitida. Se a Amazon permitir que o Fornecedor Processe as Informações da Amazon usando um Sistema de informação gerenciado pela Amazon, o Fornecedor e seus respectivos Funcionários precisarão cumprir as exigências descritas abaixo:

7.1 **Contas**. O Fornecedor assegurará que os Funcionários do Fornecedor usem apenas as contas do Sistema de informação gerenciado pela Amazon designadas pela Amazon para cada indivíduo e exigirá que os Funcionários do Fornecedor mantenham suas respectivas credenciais de acesso confidenciais e que não as compartilhem.

7.2 **Sistemas**. O Fornecedor e seus respectivos Funcionários usarão os Sistemas de informação gerenciados pela Amazon exclusivamente por meio de sistemas de computação ou processamento ou de aplicativos que:
(a) executem sistemas operacionais gerenciados pelo Fornecedor e que usem criptografia de disco completa; e,
(b) atendam às exigências das Subcláusulas 4.2 (Gerenciamento de patches), 4.4 (Defesas contra malware) e 4.9 (Segurança de rede).

7.3 **Restrições**. Salvo se aprovado antecipadamente por escrito pela Amazon, o Fornecedor e seus respectivos Funcionários não baixarão, espelharão ou armazenarão permanentemente nenhuma Informação da Amazon contida em qualquer Sistema de informação gerenciado pela Amazon, em nenhum meio.

7.4 **Encerramento da conta**. Com relação aos Funcionários que (a) não precisem mais de acesso aos Sistemas de informação gerenciados pela 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 deste Funcionário aos Sistemas de informação gerenciados pela Amazon ou notificará a Amazon para que a Amazon remova este acesso.

8. **DOMÍNIOS OU URLS DA AMAZON**. Qualquer domínio ou URL que o Fornecedor fornecer para uso exclusivo da Amazon não poderá ser emitido pelo Fornecedor ou reutilizado por terceiros por, no mínimo, 5 anos após a rescisão do Contrato.

9. DEVOLUÇÃO E EXCLUSÃO DE DADOS; DESTRUIÇÃO FORENSE DE MÍDIA.

9.1 **Devolução e exclusão de dados**. Mediante solicitação da Amazon, o Fornecedor devolverá imediatamente (mas, no máximo, em até 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 em até 30 dias após a conclusão da Finalidade permitida ou após a rescisão ou expiração do Contrato, o que ocorrer primeiro. Mediante solicitação da Amazon, o Fornecedor certificará por escrito que todas as Informações da Amazon foram excluídas. A título de esclarecimento, esta seção não se aplicará às Cópias de arquivamento de acordo com a Subcláusula 9.3.

9.2 **Sanitização de dados**. Todas as Informações da Amazon excluídas pelo Fornecedor serão excluídas de acordo com as Recomendações mínimas de sanitização contidas no NIST SP 800-88, Revisão 1, Diretrizes para sanitização de mídia (18 de dezembro de 2014, Anexo A), para purgar o tipo de dispositivo relevante. Na ausência de orientação no NIST SP 800-88 para o tipo de dispositivo relevante, o Fornecedor destruirá o dispositivo contendo Informações da Amazon de uma das seguintes maneiras: (a) purga conforme definido no NIST SP 800-88; (b) destruição conforme definido no NIST SP 800-88; ou, (c) de acordo com outras normas que a Amazon possa exigir com base na classificação e confidencialidade das Informações da Amazon.

9.3 **Cópias de arquivamento**. Se o Fornecedor for obrigado por lei a preservar cópias de arquivamento das Informações da Amazon, o Fornecedor não usará as Informações da Amazon arquivadas para nenhuma outra finalidade e

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

permanecerá vinculado a todas as suas respectivas obrigações nos termos desta Política de segurança. Qualquer Informação da Amazon arquivada precisa ser criptografada e armazenada quando o Sistema de informação coberto que hospeda ou armazena as Informações da Amazon criptografadas não tiver acesso a uma cópia das chaves usadas para criptografia. Qualquer backup "frio" ou off-line (ou seja, não disponível para uso imediato ou interativo) precisa ser armazenado em uma instalação fisicamente segura.

9.4 **Destruição forense de mídia**. Antes de descartar qualquer hardware, software ou qualquer outra mídia que contenha ou, a qualquer momento, tenha contido Informações da Amazon, o Fornecedor realizará uma destruição forense completa do hardware, software ou outra mídia de acordo com o NIST SP 800-88, Anexo A. Esta exigência de destruição não se aplicará a mídias de armazenamento às quais o Fornecedor não tenha acesso ou controle físico. Nestes casos, o Fornecedor assegurará que as Informações da Amazon sejam excluídas com segurança quando não forem mais necessárias, de acordo com as práticas recomendadas do setor.

> 9.4.1 Salvo se o Fornecedor receber o consentimento expresso por escrito da Amazon, o Fornecedor não venderá, revenderá, doará, reformará ou, de outra forma, transferirá qualquer hardware, software ou outra mídia que contenha ou, a qualquer momento, tenha contido Informações da Amazon, salvo se tiver sido forensicamente
> destruída de acordo com esta Cláusula.

10. **REVISÕES DE SEGURANÇA**. Mediante solicitação da Amazon, o Fornecedor: (a) realizará uma avaliação de risco da Amazon; (b) disponibilizará as evidências solicitadas pela Amazon para validar a conformidade do Fornecedor com esta Política de segurança; (c) permitirá que a Amazon ou o terceiro nomeado em nome da Amazon realize uma análise da conformidade do Fornecedor com esta Política de segurança; e/ou, (d) fornecerá à Amazon todos os registros mencionados na Subcláusula 4.3 no formato Open Cybersecurity Schema Framework (OCSF). Se o Fornecedor exigir que qualquer evidência seja analisada pessoalmente ou por meio de inspeção no local, em vez de disponibilizar esta evidência para análise remota da Amazon, o Fornecedor arcará com o custo da viagem e outras despesas relacionadas a esta inspeção no local. Se qualquer avaliação ou revisão identificar qualquer descoberta, o Fornecedor, às custas e despesas exclusivas do Fornecedor, tomará prontamente todas as medidas cabíveis necessárias para corrigir estas descobertas, para a satisfação razoável da Amazon e dentro de um prazo acordado.

11. **INCIDENTES DE SEGURANÇA**.

11.1 **Notificação de Incidentes de segurança**. O Fornecedor notificará a Amazon assim que possível, mas impreterivelmente até 24 horas após o Fornecedor tomar conhecimento ou acreditar, justificadamente, que houve acesso, coleta, aquisição, uso, transmissão, divulgação, corrupção ou perda não autorizada das Informações da Amazon ou de algum Sistema de informação coberto ("Incidente de segurança"). O Fornecedor enviará a notificação de Incidentes de segurança para security@amazon.com.

11.2 **Plano de resposta a incidentes**. O Fornecedor manterá um plano de resposta a incidentes por escrito e disponibilizará uma cópia deste plano à Amazon, mediante solicitação. O Fornecedor corrigirá cada Incidente de segurança em tempo hábil, de acordo com o plano de resposta a incidentes por escrito do Fornecedor e com as práticas recomendadas do setor. O Fornecedor revisará, testará e (se necessário) atualizará o plano, no mínimo, anualmente.

11.3 **Cooperação com a Amazon**. O Fornecedor: (a) auxiliará a Amazon na investigação do Incidente de segurança; (b) facilitará entrevistas com os Funcionários e outras pessoas envolvidas no Incidente de segurança ou resposta ao incidente; (c) manterá detalhes por escrito da investigação e resposta ao Incidente de segurança do Fornecedor; e, (d) disponibilizará à Amazon todos os registros, logs, arquivos, relatórios de dados, relatórios forenses, relatórios de investigação e outros materiais relevantes solicitados pela Amazon.

A tradução apresentada abaixo é apenas para fins informativos. Em caso de discrepância, inconsistência ou conflito entre esta tradução e a versão em inglês mais recente (inclusive em razão de atrasos na tradução), a versão em inglês prevalecerá.

11.4 **Notificações de terceiros**. Salvo se exigido de outra forma por lei, o Fornecedor obterá o consentimento prévio por escrito da Amazon antes de: (a) notificar qualquer terceiro (inclusive qualquer autoridade reguladora ou cliente) sobre qualquer Incidente de segurança; ou, (b) identificar a Amazon em qualquer notificação ou declaração pública sobre qualquer Incidente de segurança. Salvo se exigido de outra forma por lei, a Amazon terá o direito de determinar se a notificação do Incidente de segurança deve ser fornecida a terceiros, bem como a forma, o momento e o conteúdo dessa notificação.

12. **NOTIFICAÇÃO DE PROCESSO JUDICIAL**. Notificação de processo judicial. Exceto quando proibido por lei, se as Informações da Amazon estiverem sendo buscadas em resposta a um processo judicial ou outra lei aplicável, o Fornecedor enviará uma notificação suficiente à Amazon para permitir que a Amazon busque uma ordem de proteção ou outro recurso adequado.

13. **DEFINIÇÕES**.

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

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

13.3 "**Informações da Amazon**" refere-se a: (a) todas as Informações confidenciais da Amazon (conforme definido em qualquer outro contrato entre as partes); (b) todos os outros dados, registros, arquivos, conteúdos ou informações, em qualquer forma, adquiridas, acessadas, coletadas, recebidas, armazenadas ou mantidas pelo Fornecedor ou por suas respectivas afiliadas, da Amazon ou em nome da Amazon ou, de outra forma, relacionadas a este Contrato; e, (c) informações derivadas de (a) ou (b), mesmo se Anonimizadas.

13.4 "**Anonimizar**" refere-se a Processar qualquer dado ou informação (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.

13.5 "**Sistemas de informação cobertos**" refere-se a qualquer sistema que o Fornecedor use para Processar as Informações da Amazon.

13.6 "**Funcionários**" refere-se aos funcionários, agentes, Subcontratados e outros usuários autorizados dos sistemas e recursos de rede do Fornecedor ou do Subcontratado.

13.7 "**Processo**" refere-se à realização de qualquer operação nos dados, como acesso, uso, coleta, recebimento, armazenamento, alteração, transmissão, disseminação ou, de outra forma, disponibilização, exclusão ou destruição.

13.8 "**Fornecedor**" refere-se a cada fornecedor, vendedor ou prestador de serviços definido no Contrato e qualquer outro prestador de serviços sujeito a um Contrato.