



PADRÃO DE SEGURANÇA DA INFORMAÇÃO

Este Padrão de Segurança da Informação estabelece os requisitos de segurança da informação da Elanco Animal Health Incorporated e suas entidades afiliadas, doravante denominadas ("Elanco") para Fornecedores, no que diz respeito à confidencialidade, integridade e disponibilidade das Informações da Elanco (definidas abaixo). Quaisquer obrigações adicionais do Fornecedor relacionadas à segurança da informação da Elanco, sob qualquer acordo com a Elanco, são adicionais aos requisitos deste Padrão de Segurança da Informação.

I. Definições

"**Informações da Empresa**" significa qualquer informação confidencial ou proprietária da Elanco, incluindo qualquer informação definida como tal em qualquer acordo escrito entre o Fornecedor e a Elanco.

"**Informações da Elanco**" engloba tanto as Informações da Empresa quanto as Informações Pessoais.

"**Informações Pessoais**" significa qualquer informação relativa a uma pessoa natural identificada ou identificável; uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um número de identificação ou a um ou mais fatores específicos de sua identidade física, fisiológica, mental, econômica, cultural ou social. "Informações Pessoais" também inclui os termos "dados pessoais", "informações pessoais", "dados sensíveis", "informações pessoais sensíveis" e termos equivalentes, conforme definidos pelas leis de proteção de dados aplicáveis.

"**Processamento**" (e seus conjugados, incluindo, sem limitação, "processa", "processado" e "processando", independentemente de tais termos serem capitalizados ou não) significará qualquer operação ou conjunto de operações realizadas sobre Informações Pessoais, incluindo (sem limitação) coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

"**Sistema de Informação do Fornecedor**" significa um sistema de informação que é de propriedade ou operado por um Fornecedor ou subprocessador(es) do Fornecedor que Processa Informações da Elanco em qualquer formato, incluindo, mas não se limitando a (a) sistemas; (b) ambientes de nuvem; (c) ativos e dispositivos eletrônicos; e (e) versões em cópia impressa.

II. Requisitos

O Fornecedor deve garantir a confidencialidade, integridade e disponibilidade das Informações da Elanco, mantendo um programa abrangente de segurança da informação por escrito. O programa abrangente de segurança da informação por escrito deve ser revisado e atualizado conforme necessário, no



mínimo anualmente, ou mediante uma mudança material nos serviços prestados, e deve utilizar pelo menos os seguintes requisitos mínimos de salvaguarda, controles e procedimentos (coletivamente, as "**Salvaguardas Mínimas**"):

1. Limitar o acesso e o Processamento das Informações da Elanco a usuários autorizados e Sistemas de Informação do Fornecedor:
 - i) Identificar e autenticar as identidades dos usuários autorizados como pré-requisito para permitir o acesso aos Sistemas de Informação do Fornecedor;
 - ii) Limitar o acesso ao Sistema de Informação do Fornecedor a usuários treinados e autorizados que tenham uma necessidade comercial de conhecer para desempenhar suas funções, com requisitos de força de senha que atendam aos padrões de segurança comuns (por exemplo, ISO, NIST); e
 - iii) Fornecer treinamento periódico ao pessoal do Fornecedor que abranja segurança da informação geral e práticas seguras de processamento de dados.
2. Limitar o acesso físico aos Sistemas de Informação do Fornecedor, dispositivos, equipamentos e seus respectivos ambientes operacionais:
 - i) Acompanhar visitantes e monitorar a atividade dos visitantes, manter registros de auditoria de acesso físico e controlar e gerenciar o acesso físico aos dispositivos;
 - ii) Manter controles físicos para data centers, com acesso formalmente gerenciado com base na necessidade comercial; e
 - iii) Manter controles ambientais para data centers (por exemplo, temperatura, umidade, backup de energia).
 - iv) Monitorar, controlar e proteger as Informações da Elanco nas fronteiras externas e nas principais fronteiras internas dos Sistemas de Informação do Fornecedor, incluindo:
 - a) Fortalecer sistemas operacionais, aplicativos e dispositivos de rede, como por meio de detecção de intrusão, antivírus e anti-malware;
 - b) Aplicar patches de sistema operacional e atualizações de componentes principais após o lançamento e avaliação de patches relacionados à segurança, de acordo com os padrões de segurança comuns (por exemplo, ISO, NIST);
 - c) Proibir a autenticação de recursos de rede, plataformas, dispositivos, serviços, estações de trabalho e aplicativos por senhas padrão;
 - d) Onde razoável, implementar controle de acesso baseado em função, logon único e gerenciamento de identidade federado, e autenticação multifator;
 - e) Realizar e documentar atividades de registro de acordo com os padrões de segurança comuns (por exemplo, ISO, NIST);



- f) Criptografar dados em trânsito com procedimentos e práticas de criptografia que atendam aos padrões de segurança comuns (por exemplo, ISO, NIST);
- g) Permitir o armazenamento e a transferência de Informações da Elanco usando dispositivos de armazenamento removíveis apenas por meio de um processo documentado;
- h) Realizar varreduras periódicas dos Sistemas de Informação do Fornecedor e varreduras em tempo real de arquivos de fontes externas à medida que os arquivos são baixados ou abertos;
- i) fazer backup regularmente dos Sistemas de Informação e dados do Fornecedor, proteger adequadamente o armazenamento de backup contra perda, dano e acesso não autorizado, e testar periodicamente o armazenamento de backup quanto à segurança e viabilidade; e
- j) Documentar contas de usuário administrativo privilegiadas como diferentes das contas de usuário padrão.

O Fornecedor deve documentar, implementar e manter todas as medidas legais, operacionais, técnicas e organizacionais apropriadas para proteger contra uma Violação de Segurança de Dados (conforme definido no Acordo de Processamento de Dados). O Fornecedor deve testar ou monitorar regularmente a eficácia e a resiliência de seus controles, sistemas e procedimentos de segurança de dados.

O Fornecedor deve manter planos de continuidade de negócios e/ou recuperação de desastres documentados e operacionais, conforme razoavelmente apropriado no contexto dos serviços prestados.

O Fornecedor deve reter as Informações da Elanco apenas pelo tempo especificado no acordo aplicável, exceto na medida em que um período de retenção mais longo seja exigido por lei ou regulamentação aplicável. Ao final do contrato, o Fornecedor deve devolver ou destruir as Informações da Elanco, conforme escolha da Elanco, usando controles de descarte de ativos que atendam aos padrões de segurança comuns (por exemplo, ISO, NIST).

O Fornecedor deve manter um programa de gerenciamento de risco de terceiros que, no mínimo, exija a conformidade com as Salvaguardas Mínimas pelos subprocessadores do Fornecedor que Processam Informações da Elanco.

Na medida em que o Fornecedor construa ou forneça sistemas, software ou aplicativos para a Elanco, o Fornecedor deve:

- i) Implementar uma metodologia de Engenharia de Sistemas definida que esteja alinhada aos padrões da indústria e gerenciada por meio de políticas e procedimentos apropriados; e



**Elanco Saúde Animal**

Av. das Nações Unidas, 14401
Torre Jequitibá, 13º andar,
Chácara Santo Antônio, São
Paulo, SP, Brasil

- ii) Implementar um procedimento definido de gerenciamento de mudanças/lançamentos para mudanças de software planejadas e correções de bugs.

