Política Empresarial 7

Informação Global e Segurança de Sistemas

Finalidade

A finalidade desta Política é estabelecer o compromisso da Stryker em adotar controlos de segurança apropriados nas suas informações, sistemas e operações, de acordo com a lei aplicável.

Âmbito

Esta política aplica-se a todos os funcionários da Stryker e a terceiros (por exemplo, fornecedores, contratados, agentes) que atuem em nome da Stryker, independentemente da localização. Se qualquer disposição desta Política não estiver em conformidade com a lei local ou regional aplicável a uma entidade legal específica da Stryker, essa entidade deverá, na medida do necessário, implementar um apêndice a esta Política para cumprir a lei local ou regional, desde que a política revista esteja, na medida do possível, em conformidade com os princípios contidos nesta Política. Tal apêndice deve ser aprovado pelo CISO. Quando um apêndice local ou regional não tiver sido implementado, todas as disposições desta Política permanecerão em vigor na medida em que estejam em conformidade com a lei aplicável.

Políticas básicas

A Stryker cumprirá todas as leis que regulam a segurança dos produtos e sistemas da Stryker. Além disso, a Stryker está comprometida com as normas estabelecidas abaixo.

1. **Nomear um diretor de segurança da informação (CISO):** O CISO é responsável por estabelecer e reforçar a operação efetiva do programa de segurança global da informação da Stryker e alinhar iniciativas de segurança com programas empresariais e objetivos de negócios para a proteção de ativos, produtos, sistemas e tecnologias de informação.

2. **Implementar políticas de segurança e estruturas administrativas e de governança:** A Stryker, através dos Sistemas de Gestão da Qualidade aplicáveis, Sistema de Gestão de Segurança da Informação, normas de Governança da Informação, Normas de Uso Aceitável, Plano de Resposta a Incidentes e normas e procedimentos relacionados, implementará controlos de segurança administrativos, técnicos e físicos apropriados.

3. **Avaliar terceiros:** O processo de avaliação de segurança global deve ser concluído antes de envolver qualquer terceiro que tenha acesso às redes da Stryker ou dados eletrónicos sensíveis ou forneça soluções ou software baseados na Internet para uso interno ou uso numa oferta de produto ou serviço da Stryker.

4. **Uso de equipamentos e sistemas Stryker:** Qualquer funcionário da Stryker ou terceiro que tenha acesso aos equipamentos ou sistemas da Stryker usará esses equipamentos e sistemas em conformidade com os requisitos de uso aceitáveis aplicáveis.

Responsabilidades

É da responsabilidade de todos os funcionários da Stryker e de terceiros cumprir esta Política e todas as normas e procedimentos de implementação aplicáveis. O CISO, em coordenação com outras funções e unidades de negócios apropriadas, deve identificar todas as normas e procedimentos adicionais necessários para o cumprimento desta Política e deve preparar e implementar tais normas e procedimentos.

Conformidade

A Stryker exige que todos os funcionários e terceiros cumpram esta Política. Se tiver alguma dúvida sobre esta Política ou procedimentos relacionados ou se tiver alguma preocupação relacionada com o programa de segurança da Stryker, entre em contacto com o representante local de Recursos Humanos da Stryker, um responsável pela conformidade, um advogado ou a Linha Direta de Ética. A Stryker manterá esses relatórios confidenciais de acordo com as políticas e procedimentos da Linha Direta.