Política corporativa 7

Segurança da informação e sistemas globais

Finalidade

A finalidade desta Política é definir o compromisso da Stryker com os controles de segurança adequados para suas informações, sistemas e operações, consistentes com as leis aplicáveis.

Escopo

Esta Política se aplica a todos os funcionários da Stryker e terceiros (por exemplo, fornecedores, prestadores de serviço, agentes) que agem em nome da Stryker, independentemente do local. Se qualquer cláusula desta Política não estiver de acordo com as leis locais ou regionais aplicáveis a uma entidade jurídica específica da Stryker, essa entidade deverá, na medida do necessário, implementar um anexo a esta Política para cumprir com as leis locais ou regionais, desde que a política revisada fique, até o máximo possível, de acordo com os princípios contidos nesta Política. Esse anexo deverá ser aprovado pelo CISO. Se um anexo local ou regional não tiver sido implementado, todas as cláusulas desta Política permanecerão em vigor até onde estiverem de acordo com a lei aplicável.

Políticas básicas

A Stryker cumprirá com todas as leis que regulamentam a segurança dos produtos e sistemas da Stryker. Além disso, a Stryker está comprometida com as normas definidas a seguir.

1. **Indicar um Responsável de Segurança da Informação (Chief Information Security Officer - CISO):** O CISO é responsável por estabelecer e aplicar a operação eficaz do programa de segurança da informação global da Stryker e alinhar as iniciativas de segurança com os programas e objetivos comerciais da empresa para proteção de ativos de informações, produtos, sistemas e tecnologias.

2. **Implementar políticas de segurança e estruturas de governança e administrativas:** A Stryker irá, por meio de sistemas de gerenciamento de qualidade, sistemas de gerenciamento de segurança da informação, padrões de governança de informações, padrões de uso aceitável, plano de resposta a incidentes e normas e procedimentos relacionados, implementar controles de segurança administrativos, técnicos, físicos e de segurança adequados.

3. **Avaliar terceiros:** O processo de avaliação de segurança global deverá ser concluído, antes de envolver qualquer terceiro que tenha acesso a redes da Stryker, ou a dados confidenciais ou forneça soluções ou software da internet para uso interno ou uso em um produto ou oferta de serviço da Stryker.

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

Responsabilidades

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

Conformidade

A Stryker exige que todos os funcionários e terceiros cumpram esta Política. Se você tiver dúvidas sobre esta Política ou procedimentos relacionados ou se tiver preocupações relacionadas ao programa de segurança da Stryker, entre em contato com um representante local de Recursos Humanos, o Responsável de Conformidade (Compliance Officer), Consultor Jurídico ou com a Linha direta de ética da Stryker. A Stryker irá tratar esses relatos como confidenciais, de acordo com as políticas e procedimentos da Linha direta.