Política corporativa 7
Información global y Seguridad de sistemas

Propósito

El propósito de esta Política es establecer el compromiso de Stryker con los controles de seguridad apropiados en su información y sus sistemas y operaciones, consecuentes con la ley aplicable.

Alcance

Esta Política rige para todos los empleados y terceros de Stryker (por ejemplo, proveedores, contratistas, agentes) que actúen en nombre de Stryker, independientemente de su ubicación. Si alguna disposición de esta Política no cumple con las leyes locales o regionales aplicables a una persona jurídica de Stryker específica, esa persona jurídica deberá, en la medida en que sea necesario, redactar un apéndice a esta Política para cumplir con las leyes locales o regionales, siempre y cuando esa política corregida esté en consonancia, en la mayor medida posible, con los principios consagrados en esta Política. Dicho apéndice deberá ser aprobado por el Director de seguridad de la información (Chief Information Security Officer, CISO). Cuando no se haya redactado un apéndice local o regional, todas las disposiciones de esta Política seguirán vigentes en la medida en que cumplan con las leyes aplicables.

Políticas básicas

Stryker cumplirá con todas las leyes que regulan la seguridad de los productos y sistemas de Stryker. Además, Stryker está comprometida con las normas que se establecen a continuación.

1. **Designación de un Director de seguridad de la información (CISO):** El CISO es responsable de establecer y garantizar la operación efectiva del programa de seguridad de información global de Stryker y de alinear las iniciativas de seguridad con los programas corporativos y los objetivos comerciales para la protección de los activos de información, los productos, los sistemas y las tecnologías.

2. **Implementación de políticas de seguridad y de estructuras administrativas y de gobernanza:** Stryker, a través de los Sistemas de Gestión de Calidad, el Sistema de Gestión de Seguridad de la Información, los Estándares de Gobierno de la Información, los Estándares de Uso Aceptable, el Plan de Respuesta a Incidentes, y los estándares y procedimientos relacionados, implementará los controles administrativos, técnicos y de seguridad física apropiados.

3. **Evaluación a terceros:** Se debe realizar el proceso de evaluación de seguridad global antes de la participación de un tercero que tenga acceso a las redes o los datos sensibles electrónicos de Stryker, o proporcione soluciones basadas en Internet o software para uso interno o se utilice en una oferta de servicios o productos de Stryker.

4. **Uso de los equipos y sistemas de Stryker:** Cualquier empleado de Stryker o tercero que tenga acceso a los equipos o sistemas de Stryker utilizará dichos equipos o sistemas de conformidad con los requisitos de uso aceptable que correspondan.

Responsabilidades

Es responsabilidad de todos los empleados de Stryker y terceros cumplir con esta Política y con todas las normas y los procedimientos de implementación aplicables. El CISO, en coordinación con otras funciones y unidades de negocios apropiadas, deberá identificar cualquier estándar y procedimiento adicional necesario para el cumplimiento de esta Política, y deberá preparar e implementar dichos estándares y procedimientos.

Cumplimiento

Stryker exige a todos los empleados y a los terceros el cumplimiento de esta Política. Si tiene alguna pregunta acerca de esta Política o los procedimientos relacionados, o si tiene una inquietud con respecto al programa de seguridad de Stryker, comuníquese con el representante local de Recursos Humanos, un funcionario de cumplimiento, asesor legal o la línea directa de ética de Stryker. Stryker mantendrá esos informes de manera confidencial de conformidad con las políticas y procedimientos de la línea directa.