Corporate Policy 7

Global Information and Systems Security

Purpose

The Purpose of this Policy is to set forth Stryker's commitment to appropriate security controls in its information, systems and operations consistent with applicable law.

Scope

This Policy applies to all Stryker employees and third parties (e.g., vendors, contractors, agents) acting on behalf of Stryker regardless of location. If any provision of this Policy does not comply with local or regional law applicable to a specific Stryker legal entity, that entity shall, to the extent necessary, implement an appendix to this Policy to comply with local or regional law, provided that the revised policy will to the greatest extent possible conform with the principles contained within this Policy. Such appendix shall be approved by the CISO. Where a local or regional appendix has not been implemented, all provisions of this Policy will remain in effect to the extent compliant with applicable law.

Basic policies

Stryker will comply with all laws regulating the security of Stryker's products and systems. In addition, Stryker is committed to the standards set forth below.

1. **Appoint a chief information security officer (CISO):** The CISO is responsible for establishing and enforcing effective operation of Stryker's global information security program and aligning security initiatives with enterprise programs and business objectives for the protection of information assets, products, systems, and technologies.

2. **Implement security policies and administrative and governance structures:** Stryker will, through the applicable Quality Management Systems, Information Security Management System, Information Governance standards, Acceptable Use standards, Incident Response Plan, and related standards and procedures, implement appropriate administrative, technical, and physical security controls.

3. **Assess third parties:** The global security assessment process must be completed prior to engaging any third party who has access to Stryker's networks or electronic sensitive data or provides internet-based solutions or software for internal use or use in a Stryker product or service offering.

4. **Use of Stryker equipment and systems:** Any Stryker employee or third party who has access to Stryker's equipment or systems will use such equipment and systems in compliance with applicable acceptable use requirements.

Responsibilities

It is the responsibility of all Stryker employees and third parties to comply with this Policy and all applicable implementing standards and procedures. The CISO, in coordination with other appropriate functions and business units, shall identify any additional standards and procedures necessary for compliance with this Policy and shall prepare and implement such standards and procedures.

Compliance

Stryker requires all employees and third parties to comply with this Policy. If you have a question about this Policy or related procedures or if you have a concern regarding Stryker's security program, please contact Stryker's local Human Resources representative, a compliance officer, legal counsel or the Ethics Hotline. Stryker shall keep such reports confidential in accordance with Hotline policies and procedures.