公司政策 7
全球信息和系统安全

目的

本政策旨在阐明 Stryker 会遵守适用的法律，承诺在其信息、系统和运营中实施适当的安全控制措施。

适用范围

本政策适用于所有 Stryker 员工和代表 Stryker 行事的第三方（如供应商、承包商、代理），无论其办公地点为何。
如果本政策的某项规定不符合适用于特定 Stryker 法律实体的当地或地区法律，则该实体应在必要范围内实施本政策的附则，以符合当地或地区法律，前提是修订后的政策在最大范围内符合本政策所含的原则。此类附则应由 CISO 批准。在尚未实施当地或地区附则的地方，本政策的所有规定将在符合适用法律的范围内保持有效。

基本政策

Stryker 将遵守管控 Stryker 产品和系统安全性的所有法律。除此之外，Stryker 还致力于遵守下面规定的标准。

1. **委任一名首席信息安全管理官 (CISO)：**CISO 负责制定并有效执行 Stryker 的全球信息安全计划，并将安全举措与企业计划和业务目标协调一致，以保护信息资产、产品、系统和技术。

2. **实施安全政策和行政管理结构：**Stryker 将通过适用的质量管理体系、信息安全管理系统、信息治理标准、合格使用标准、事件响应计划和相关标准及规程，实施适当的行政、技术和物理安全控制措施。

3. **评估第三方：**在聘请任何第三方，授权其访问 Stryker 的网络或电子敏感数据之前，或者提供基于互联网的解决方案或软件以供内部使用或用于 Stryker 产品或服务供应之前，必须完成全球安全评估流程。

4. **Stryker 设备和系统的使用：**任何 Stryker 员工或有权访问 Stryker 的设备或系统的第三方都将按照适用的合格使用标准来使用此类设备和系统。

责任

所有 Stryker 员工和第三方都有责任遵守本政策及所有使用的实施标准和规程。CISO 应与其他相关职能部门和业务部门进行协调，确定遵守本政策所需的任何其他标准和规程，并准备和实施此类标准和规程。

合规性

Stryker 要求所有员工和第三方均遵守本政策。如果您对本政策或相关规程有问题，或者对于 Stryker 的安全计划有疑虑，请联系 Stryker 的当地人力资源代表、合规官、法律顾问或道德热线。Stryker 应按照热线政策和流程对此类报告保密。