企業政策 7
全球資訊與系統安全

目的

本政策的目的在於闡述 Stryker 的承諾，即根據適用法律，在資訊、系統和營運中採取適當的安全控制措施。

範圍

本政策適用於任何地點的所有 Stryker 員工以及代表 Stryker 行事的第三方 (例如廠商、承包商、代理商)。倘若本政策的任何條款與適用於特定 Stryker 法律實體的當地或地區法律不符，則該實體應在必要時實施本政策的附錄內容以符合當地或地區法律，前提是修訂後的政策將在最大限度上符合本政策中包含的原則。此類附錄應獲得 CISO 的核准。如果當地或地區附錄尚未實施，則本政策的所有條款將在符合適用法律的情況下持續生效。

基本政策

Stryker 將遵守規範 Stryker 產品與系統安全性的所有法律。此外，Stryker 致力於符合下列標準。

1. **指派資訊安全長 (CISO)：**CISO 有責任建立並強制有效執行 Stryker 的全球資訊安全計劃，並確保安全措施符合相應的企業計劃與業務目標，以保護資訊資產、產品、系統及技術。

2. **實施安全政策以及管理與治理結構：**Stryker 將會透過適用的品質管理系統、資訊安全管理系統、資訊治理標準、合理的使用標準、事故應變計劃及相關標準和程序，實施適當的管理、技術及實體安全控制措施。

3. **評估第三方：**在聘請擁有 Stryker 網路或電子敏感資料存取權限的任何第三方，或提供網路解決方案或軟體以供內部使用或用於 Stryker 產品或服務之前，必須完成全球安全評估流程。

4. **Stryker 設備與系統的使用：**擁有 Stryker 設備與系統存取權限的任何 Stryker 員工或第三方在使用此類設備與系統時應遵守適用的合理的使用規定。

責任

所有 Stryker 員工與第三方皆有責任遵守本政策以及所有適用的實施標準與程序。CISO 應與其他適當的職能和業務單位協調，確認遵守本政策所需的任何其他標準與程序，並應制定及實施此類標準與程序。

合規

Stryker 要求所有員工及第三方遵守本政策。倘若您對本政策或相關程序有任何問題，或者您對 Stryker 的安全計劃有任何疑慮，請聯絡 Stryker 當地的人力資源代表、法規遵循主管、法律顧問或道德熱線。Stryker 應根據熱線政策與程序，對此類報告保密。