기업 정책 7
글로벌 정보 및 시스템 보안

목적

본 정책은 Stryker 의 정보, 시스템 및 운영에 있어서 해당 법률에 부합하는 적절한 보안 통제에 관한 Stryker 의 약속을 규정합니다.

범위

본 정책은 위치에 관계없이 Stryker 를 대신하여 활동하는 모든 Stryker 직원 및 제 3 자(예: 공급업체, 계약업체, 대리인)에 적용됩니다. 본 정책의 어떠한 조항이 특정 Stryker 법인에 적용되는 현지 또는 지역 법률을 준수하지 않는 경우, 본 정책에 포함된 원칙을 최대한의 범위까지 준수하며 현지 또는 지역 법률을 준수하는 본 정책의 부록을 시행해야 합니다. 이러한 부록은 CISO 의 승인을 받아야 합니다. 현지 또는 지역 부록을 시행한 적이 없는 경우에는 본 정책의 모든 조항이 적용 가능한 법률에 부합하는 범위까지 효력을 발휘합니다.

기본 정책

Stryker 는 Stryker 의 제품 및 시스템의 보안을 규제하는 모든 법률을 준수합니다. 뿐만 아니라 Stryker 는 아래에 규정된 표준을 준수하기 위해 전념합니다.

1. **최고 정보 보안 책임자(CISO) 임명:** CISO는 Stryker의 글로벌 정보 보안 프로그램의 효과적인 운영을 수립하고 시행하며 정보 자산, 제품, 시스템, 기술을 보호하기 위해 기업 프로그램 및 사업 목표에 맞추어 보안 이니셔티브를 조정할 책임이 있습니다.

2. **보안 정책 및 관리 및 거버넌스 구조 구현:** Stryker는 적용 가능한 품질 관리 시스템, 정보 보안 관리 시스템, 정보 거버넌스 표준, 허용 가능한 사용 표준, 사고 대응 계획, 관련 표준 및 절차를 통해 적절한 관리, 기술, 물리적 보안 통제를 구현합니다.

3. **제3자 평가:** Stryker의 네트워크 또는 민감한 전자 데이터에 액세스 권한이 있거나 Stryker 제품이나 서비스 오퍼링에서 내부적으로 사용 또는 사용하기 위한 인터넷 기반 솔루션 또는 소프트웨어를 제공하는 어떠한 제3자라도 참여시키는 경우 그에 앞서 글로벌 보안 평가 프로세스를 완료해야 합니다.

4. **Stryker 장비 및 시스템의 사용:** Stryker의 장비 또는 시스템에 액세스 권한이 있는 모든 Stryker 직원 또는 제3자는 적용 가능하고 허용 가능한 사용 요건을 준수하는 장비와 시스템을 사용합니다.

책임

Stryker의 모든 직원 및 제3자는 본 정책과 시행하고 있는 적용 가능한 모든 표준 및 절차를 준수할 책임이 있습니다. CISO는 본 정책을 준수하기 위해 필요한 부가적인 표준과 절차를 파악해야 하며 해당 사업부 및 업무 부서와의 협력을 통해 이러한 표준과 절차를 마련하고 이행해야 합니다.

규정 준수

Stryker 는 모든 직원 및 제 3 자가 본 정책을 준수하도록 요구합니다. 본 정책 또는 관련 절차에 질문이 있거나 Stryker 의 보안 프로그램과 관련하여 우려 사항이 있는 경우에는 Stryker 의 현지 인사 담당자, 규정 준수 책임자, 법률 자문 또는 윤리 핫라인으로 문의하여 주시길 바랍니다. Stryker 는 핫라인 정책 및 절차에 따라 이러한 보고를 기밀로 유지해야 합니다.