Kurumsal Politika 7

Küresel Bilgi ve Sistem Güvenliği

Amaç

Bu Politikanın Amacı Stryker'in bilgi, sistemler ve operasyonlarına ilişkin yürürlükteki yasalarla tutarlı güvenlik kontrollerini uygun hale getirmek için Stryker'ın taahhüdünü ortaya koymaktır.

Kapsam

Bu Politika konumdan bağımsız olarak tüm Stryker çalışanları ve üçüncü taraflar (örn., satıcılar, yükleniciler, vekiller) için geçerlidir. Bu Politikanın herhangi bir hükmü belirli bir Stryker tüzel kişiliği için geçerli olan yürürlükteki yerel veya bölgesel yasa ile uyumlu olmadığı durumlarda, o tüzel kişilik, gerektiği ölçüde, gözden geçirilmiş politikanın bu Politika içinde yer alan ilkelere uyması mümkün olması kaydıyla, yerel veya bölgesel yasalara uymak için bu Politikanın bir ekini oluşturur. Böyle bir ek CISO tarafından onaylanacaktır. Yerel veya bölgesel ekin oluşturulmadığı hallerde, bu Politikanın tüm hükümleri yürürlükteki yasaya uygun ölçüde yürürlükte kalacaktır.

Temel politikalar

Stryker, Stryker'ın ürünlerinin ve sistemlerinin güvenliğini düzenleyen tüm yasalarla uyumlu davranacaktır. Ek olarak, Stryker aşağıda otaya konulan standartları taahhüt eder.

1. **Baş bilgi güvenliği yetkilisi (CISO) atamak:** CISO, Stryker'ın küresel bilgi güvenliği programının etkili işletiminden kurulmasından ve zorunlu kılınmasından ve bilgi varlıklarının, ürünlerin, sistemlerin ve teknolojilerin korunması için güvenlik girişimlerinin kurumsal programlarla ve iş hedefleriyle uyumlandırılmasından sorumludur.

2. **Güvenlik politikalarını ve idari ve yönetimsel yapıları uygulamak:** Stryker geçerli Kalite Yönetim Sistemleri, Bilgi Güvenliği Yönetim Sistemi, Bilgi Yönetim standartları, Kabul Edilebilir Kullanım standartları, Olay Yanıt Planı ve ilgili standartlar ve prosedürler aracılığı ile uygun idari, teknik ve ve fiziksel güvenlik kontrollerini uygulayacaktır.

3. **Üçüncü tarafları incelemek:** Stryker'ın ağlarına veya elektronik duyarlı verilerine erişmeden veya dahili kullanım için internet tabanlı çözümler veya yazılım üretmeden veya Stryker ürününde veya sunduğu hizmetinde kullanmadan önce herhangi bir üçüncü tarafın küresel güvenlik değerlendirmesi tamamlanmalıdır.

4. **Stryker donanım ve sistemlerinin kullanımı:** Stryker donanım veya sistemlerine erişimi olan herhangi bir Stryker çalışanı veya üçüncü taraf bu tür donanımları ve sistemleri geçerli olan kabul edilebilir gereklilikler ile uyum içinde kullanacaktır.

Sorumluluklar

Bu Politika ve tüm geçerli uygulanan standartlar ve prosedürler ile uyumlu olmak tüm Stryker çalışanlarının ve üçüncü tarafların sorumluluğundadır. CISO, ilgili diğer fonksiyonlar ve iş birimleriyle koordineli olarak, bu Politika ile uyum için gereken her türlü ek standartları ve prosedürleri tanımlayacak ve bu tür standartları ve prosedürleri hazırlayacak ve uygulayacaktır.

Uyum

Stryker tüm çalışanları ve üçüncü taraflardan bu Politika ile uyum sağlamalarını talep eder. Bu Politika veya ilgili prosedürler ile ilgili sorunuz varsa veya Stryker'ın güvenlik programı ile ilgili endişeniz mevcutsa, lütfen Stryker'ın yerel İnsan Kaynakları temsilcisi, uyumluluk yetkilisi, hukuk müşaviri veya Etik Yardım Hattı ile iletişime geçin. Stryker bu tür raporları Yardım Hattı politikaları ve prosedürlerine uygun olarak saklayacaktır.