Företagspolicy 7
Global information och systemsäkerhet

Syfte

Syftet med denna policy är att beskriva Strykers åtagande att använda lämpliga säkerhetskontroller i sin information, sina system och verksamheter som överensstämmer med tillämplig lag.

Omfattning

Denna policy gäller för alla anställda på Stryker och tredje parter (t.ex. säljare, underleverantörer, representanter) som agerar på Strykers vägnar, oavsett var. Om någon del av denna policy inte efterlever lokal eller regional lagstiftning vad gäller en av Strykers specifika juridiska enheter ska denna enhet, i den utsträckning som krävs, införliva en bilaga i denna policy för att efterleva den lokala eller regionala lagstiftningen så länge den reviderade policyn i största möjliga utsträckning överensstämmer med principerna i denna policy. Informationssäkerhetschefen måste godkänna en sådan bilaga. Där en lokal eller regional bilaga inte har implementerats gäller alla provisionerna i denna i den utsträckning de efterlever tillämplig lagstiftning.

Grundläggande policyer

Stryker kommer att följa alla lagar som reglerar Strykers produkters och systems säkerhet. Utöver detta åtar sig Stryker att leva upp till de standarder som beskrivs nedan.

1. **Utse en informationssäkerhetschef (CISO):** Den centrala informationssäkerhetschefen har ansvaret för att etablera och upprätthålla effektiv drift av Strykers globala säkerhetssystem och se till att säkerhetsinitiativ överensstämmer med företagsprogram och företagets mål för att skydda informationstillgångar, produkter, system och teknologier.

2. **Implementera säkerhetspolicyer och strukturer för administrations- och styrningsstrukturer:** Stryker kommer med hjälp av kvalitetshanteringssystem, system för hanteringen av informationssäkerhet, information om tillämpningen av standarder, godtagbara användningsstandarder, incidenthanteringsplan och relaterade standarder och procedurer implementera lämpliga administrativa, tekniska och fysiska säkerhetskontroller.

3. **Utvärdera tredje parter:** Den globala säkerhetsutvärderingsprocessen måste avslutas innan en tredje part får tillgång till Strykers nätverk eller känslig elektronisk data eller tillhandahåller internetbaserade lösningar eller mjukvara för intern användning eller användning i en Strykerprodukt eller tjänste-erbjudande.

4. **Användning av Strykers utrustning och system:** Alla anställda hos Stryker eller tredje part som har tillgång till Strykers utrustning och system ska använda sådan utrustning och system i enlighet med tillämpliga krav för acceptabel användning.

Ansvarsområden

Alla Strykers anställda och tredje parter ansvarar för att efterleva denna policy och alla tillämpliga implementeringsstandarder och procedurer. Den centrala informationssäkerhetschefen ska identifiera ytterligare standarder och procedurer som är nödvändiga för att efterleva denna policy och tillsammans med tillämpliga affärsenheter och funktioner koordinera när det gäller att förbereda och implementera sådana standarder och procedurer.

Efterlevnad

Stryker kräver att alla anställda och tredje parter efterlever denna policy. Om du har frågor om denna policy eller relaterade procedurer eller om det finns något med Strykers säkerhetsprogram som oroar dig, vänligen kontakta Strykers personalavdelning, en compliance officer, juridiskt ombud eller vår Ethics Hotline. Stryker kommer att se till att sådana rapporter förblir konfidentiella i enlighet med Hotline policyer och procedurer.