Bedrijfsbeleid 7

Wereldwijde informatie- en systeembeveiliging

Doel

Het doel van dit beleid is het uiteenzetten van de inspanningen van Stryker om te zorgen voor passende beveiligingscontroles voor de informatie, systemen en bedrijfsactiviteiten die in overeenstemming zijn met de toepasselijke wetgeving.

Toepassingsgebied

Dit beleid is van toepassing op alle werknemers en derden (zoals verkopers, contractanten en vertegenwoordigers) die namens Stryker handelen, ongeacht op welke locatie ze dat doen. Ingeval enige bepaling van dit beleid niet mocht voldoen aan de lokale of regionale wetgeving waar deze van toepassing is op een bepaalde rechtspersoon van Stryker, dan dient deze rechtspersoon, voor zover nodig, een bijlage aan dit beleid toe te voegen om aan de lokale of regionale wetgeving te voldoen, op voorwaarde dat het herziene beleid zoveel mogelijk overeenstemt met de principes die in dit beleid worden uiteengezet. Die bijlage dient door de centrale informatiebeveiligingsfunctionaris (CISO) te worden goedgekeurd. Indien er geen bijlage met betrekking tot lokale of regionale wetgeving is bijgevoegd, blijven alle bepalingen van dit beleid van kracht voor zover deze in overeenstemming zijn met de toepasselijke wetgeving.

Basisbeleid

Stryker leeft alle wetgeving na inzake de beveiliging van haar producten en systemen. Bovendien is Stryker toegewijd aan de hieronder uiteengezette normen.

1. **De aanstelling van een centrale informatiebeveiligingsfunctionaris (CISO):** De centrale informatiebeveiligingsfunctionaris (CISO) is verantwoordelijk voor het tot stand brengen en handhaven van een effectief werkend, wereldwijd beveiligingsprogramma van Stryker en het afstemmen van beveiligingsinitiatieven op bedrijfsprogramma's en zakelijke doelstellingen ter bescherming van informatiemiddelen, producten, systemen en technologieën.

2. **De implementatie van beveiligingsbeleid alsmede van administratieve en bestuurlijke structuren:** Stryker zal, door middel van de toepasselijke kwaliteitsbeheersystemen, het informatiebeveiligingsbeheersysteem (Information Security Management System), de normen voor aanvaardbaar gebruik, het Incident Response Plan en de aanverwante normen en procedures, passende administratieve, technische en fysieke beveiligingsmaatregelen implementeren.

3. **De uitvoering van veiligheidsbeoordelingen op derden:** Het ‘global security assessment process’ (wereldwijde veiligheidsbeoordelingsproces) dient te zijn afgerond voorafgaand aan eventuele samenwerkingen met een derde die toegang krijgt tot de netwerken of gevoelige elektronische gegevens van Stryker of oplossingen die op het internet zijn aangesloten of software voor intern gebruik aanbiedt of voor gebruik in combinatie met een Stryker-product of -dienstenaanbod.

4. **Het gebruik van apparatuur en systemen van Stryker:** Een werknemer van Stryker of een derde die toegang heeft tot de apparatuur of de systemen van Stryker zal deze apparatuur en systemen in overeenstemming met de toepasselijke vereisten op het gebied van aanvaardbaar gebruik (Acceptable Use Policy) gebruiken.

Verantwoordelijkheden

Het is de verantwoordelijkheid van alle werknemers van Stryker en van derden om dit beleid en alle toepasselijke implementatienormen en -procedures na te leven. De CISO zal, in coördinatie met andere passende functies en bedrijfseenheden, eventuele aanvullende normen en procedures identificeren die noodzakelijk zijn voor de naleving van dit beleid en zal dergelijke normen en procedures voorbereiden en implementeren.

Naleving

Stryker verplicht al haar werknemers en alle derden om dit beleid na te leven. Als u een vraag hebt over dit beleid of aanverwante procedures of als u een zorg wilt bespreken aangaande het beveiligingsprogramma van Stryker, neem dan contact op met de plaatselijke HR-vertegenwoordiger van Stryker, een nalevingsfunctionaris, een juridisch adviseur of onze ethische hulplijn (Ethics Hotline). Stryker verbindt zich ertoe dergelijke meldingen in overeenstemming met het beleid en de procedures van de hulplijn vertrouwelijk te behandelen.