Selskapspolicy 7
Global informasjon og systemsikkerhet

Formål

Formålet med denne policyen er å fastslå Strykers forpliktelse til hensiktsmessige sikkerhetskontroller i sin informasjon, systemer og virksomhet i samsvar med gjeldende lov.

Rekkevidde

Denne policyen gjelder alle Strykers ansatte og tredjeparter (for eksempel leverandører, kontraktører, agenter) som handler på vegne av Stryker, uansett sted. Dersom noen bestemmelse i denne policyen ikke overholder lokal eller regional lov som gjelder for en bestemt juridisk enhet innen Stryker, skal denne enheten, i den utstrekning det er nødvendig, gjennomføre et tillegg til denne policyen for å overholde lokal eller regional lov, forutsatt at den reviderte policyen i størst mulig grad er i samsvar med prinsippene i denne policyen. Et slikt tillegg skal godkjennes av CISO. Dersom et lokalt eller regionalt tillegg ikke er iverksatt, vil alle bestemmelser i denne policyen fortsatt gjelde i den grad det er i samsvar med gjeldende lov.

Grunnleggende policyer

Stryker vil overholde alle lover som regulerer sikkerheten til Strykers produkter og systemer. Dessuten er Stryker forpliktet til standardene som er beskrevet nedenfor.

1. **Utpeke en informasjonssikkerhetsleder (CISO):** CISO er ansvarlig for å etablere og håndheve effektiv drift av Strykers globale informasjonssikkerhetsprogram og tilrettelegge sikkerhetsinitiativer med bedriftsprogrammer og forretningsmessige mål for beskyttelse av informasjonsmidler, produkter, systemer og teknologier.

2. **Iverksette sikkerhetspolicyer, administrative strukturer og styringsstrukturer:** Stryker vil gjennom relevante kvalitetsstyringssystemer, informasjonssikkerhetsstyringssystem, informasjonsstyringssystemer, akseptable bruksstandarder, hendelseresponsplan og tilhørende standarder og prosedyrer, iverksette hensiktsmessige administrative, tekniske og fysiske sikkerhetskontroller.

3. **Vurdere tredjeparter:** Den globale sikkerhetsvurderingsprosessen må være fullført før det engasjeres en tredjepart som har tilgang til Strykers nettverk eller elektroniske følsomme data, eller leverer internettbaserte løsninger, eller programvare for intern bruk eller for bruk i et Stryker-produkt eller tjenestetilbud.

4. **Bruk av Stryker-utstyr og -systemer:** Enhver Stryker-ansatt eller tredjepart som har tilgang til Strykers utstyr eller systemer skal bruke utstyr og systemer som er i samsvar med gjeldende bruksbehov.

Ansvar

Det er ansvaret til alle Stryker-ansatte og tredjeparter å overholde disse retningslinjene og alle gjeldende iverksettingsstandarder og prosedyrer. CISO skal, i samarbeid med andre passende funksjoner og forretningsenheter, identifisere eventuelle tilleggsstandarder og prosedyrer som er nødvendige for å overholde denne policyen og skal koordinere med de aktuelle forretningsenhetene og funksjonene ved utarbeidelse og gjennomføring av slike standarder og prosedyrer.

Samsvar

Stryker krever at alle ansatte og tredjeparter overholder denne policyen. Dersom du har spørsmål om denne policyen eller relaterte prosedyrer, eller dersom du har et problem i forbindelse med Strykers sikkerhetsprogram, ta kontakt med Strykers lokale HR-representant, en overholdelsesansvarlig, juridisk rådgiver eller etikk-direktelinjen. Stryker skal holde disse rapportene konfidensielle i henhold til direktelinjepolicyer og -prosedyrer.