Yhtiön käytäntö 7

Maailmanlaajuinen tieto- ja järjestelmäturva

Tarkoitus

Tämän käytännön tarkoitus on määrittää Strykerin sitoumus asianmukaisten turvavalvontatoimenpiteiden toteuttamiseen sen tietojen, järjestelmien ja toimintojen osalta sovellettavan lainsäädännön mukaisesti.

Soveltamisala

Tämä käytäntö koskee kaikkia Strykerin työntekijöitä sekä kolmansia osapuolia (kuten tavarantoimittajat, alihankkijat ja asiamiehet), jotka toimivat Strykerin puolesta maantieteellisestä sijainnista riippumatta. Mikäli jokin tämän käytännön ehto on ristiriidassa johonkin tiettyyn Strykerin oikeushenkilöön sovellettavan paikallisen tai alueellisen lainsäädännön kanssa, kyseisen oikeushenkilön tulee tarvittavassa laajuudessa laatia liite tähän käytäntöön, jotta se noudattaisi paikallista tai alueellista lainsäädäntöä, edellyttäen että tarkistettu käytäntö noudattaa mahdollisimman suuressa määrin tämän käytännön sisältämiä periaatteita. CISO:n tulee hyväksyä edellä kuvatun kaltainen liite. Mikäli paikallista tai alueellista liitettä ei ole laadittu, kaikki tämän käytännön kohdat pysyvät voimassa sovellettavan lainsäädännön sallimassalaajuudessa.

Peruskäytännöt

Stryker noudattaa kaikkia lakeja, joilla säädetään Strykerin tuotteiden ja järjestelmien turvallisuudesta. Lisäksi Stryker on sitoutunut noudattamaan jäljempänä asetettuja standardeja.

1. **Tietoturvajohtajan (chief information security officer, CISO) nimittäminen:** CISO on vastuussa Strykerin maailmanlaajuisen tietoturvallisuusohjelman tehokkaasta käyttöönotosta ja täytäntöönpanosta sekä turvallisuusaloitteiden linjauksesta yhtymä- ja liiketoimintatavoitteisiin tieto-omaisuuden, tuotteiden, järjestelmien ja teknologioiden suojaamiseksi.

2. **Turvallisuuskäytäntöjen ja hallinnollisten sekä johtamisrakenteiden toteuttaminen:** Sovellettavien laadunhallintajärjestelmien, tietoturvan hallintajärjestelmän, tietojen hallintastandardien, hyväksyttävän käytön standardien, onnettomuuksiin vastaamissuunnitelman ja siihen liittyvien standardien ja menettelyjen avulla Stryker toteuttaa asianmukaiset hallinnolliset, tekniset ja fyysiset turvavalvontatoimenpiteet.

3. **Kolmansien osapuolten arviointi:** Maailmanlaajuinen turvallisuusarviointiprosessi täytyy suorittaa ennen yhteistyön aloittamista minkään sellaisen kolmannen osapuolen kanssa, jolla on pääsy Strykerin verkkoihin tai elektronisessa muodossa olevaan arkaluontoiseen tietoon tai joka tarjoaa internetpohjaisia ratkaisuja tai ohjelmistoja sisäiseen käyttöön tai käytettäväksi osana Strykerin tuotetta tai palvelua.

4. **Strykerin laitteiden ja järjestelmien käyttö:** Kenen tahansa Strykerin työntekijän tai kolmannen osapuolen, jolla on pääsy Strykerin laitteisiin tai järjestelmiin, tulee käyttää niitä sovellettavien hyväksyttävän käytön vaatimusten mukaisesti.

Vastuut

Kaikkien Strykerin työntekijöiden ja kolmansien osapuolten vastuulla on noudattaa tätä Käytäntöä ja kaikkia sovellettavia toteutusstandardeja ja menettelyjä. CISO tunnistaa kaikki lisästandardit ja menettelyt, jotka ovat tarpeen tämän käytännön noudattamiseksi, ja koordinoi yhdessä soveltuvien liiketoimintayksikköjen ja toimintojen kanssa kyseisten standardien ja menettelyjen laatimisen ja käyttöönoton.

Vaatimustenmukaisuus

Stryker vaatii kaikkia työntekijöitä ja kolmansia osapuolia noudattamaan tätä käytäntöä. Mikäli sinulla on kysyttävää tästä käytännöstä tai siihen liittyvistä menettelyistä tai mikäli sinulla Strykerin turvallisuusohjelmaa koskeva huolenaihe, ota yhteyttä Strykerin paikalliseen henkilöstöosaston edustajaan, vaatimustenmukaisuusvastaavaan, oikeudelliseen neuvonantajaan tai Ethics Hotlineen. Stryker pitää nämä raportit luottamuksellisena palvelupuhelimen käytäntöjen ja menettelyjen mukaisesti.