Politica aziendale 7

Sicurezza globale delle informazioni e dei sistemi

Scopo

Lo scopo di questa politica è enunciare l'impegno di Stryker alla realizzazione di idonei controlli di sicurezza sulle proprie informazioni, sistemi e operazioni in conformità alle leggi applicabili.

Campo di applicazione

Questa politica si applica a tutti i dipendenti di Stryker e alle terze parti (per es., fornitori, contraenti, agenti) che agiscono per conto di Stryker, indipendentemente dal luogo in cui si trovano. Se una qualsiasi disposizione di questa politica non è conforme alla legge locale o regionale applicabile a una particolare entità giuridica di Stryker, tale entità deve, nella misura necessaria, compilare un'appendice alla presente politica per conformarsi alla legge locale o regionale, a condizione che la nuova politica sia conforme per quanto possibile ai principi contenuti all'interno della presente. Tale appendice deve essere approvata dal CISO. Laddove non sia stata compilata un'appendice locale o regionale, tutte le disposizioni della presente politica rimangono in vigore in misura conforme alle leggi applicabili.

Politiche fondamentali

Stryker si attiene a tutte le leggi che regolano la sicurezza dei propri prodotti e sistemi. Inoltre Stryker si impegna ad applicare le norme riportate di seguito.

1. **Nomina di un responsabile della sicurezza informatica (chief information security officer, CISO):** Il CISO è responsabile della creazione e dell'implementazione efficace delle azioni previste dal programma di sicurezza informatica globale di Stryker e dell'allineamento delle iniziative di sicurezza con i programmi aziendali e gli obiettivi commerciali per la protezione delle risorse informatiche, dei prodotti, dei sistemi e delle tecnologie.

2. **Realizzazione delle politiche sulla sicurezza e delle strutture amministrative e gestionali:** Tramite i relativi Sistemi di gestione della qualità, il Sistema di gestione della sicurezza informatica, gli standard di Governance delle informazioni, gli standard di Uso accettabile, il Piano di intervento in caso di incidenti e le relative norme e procedure, Stryker realizzerà idonei controlli sulla sicurezza amministrativa, tecnica e fisica.

3. **Valutazione delle terze parti:** Il processo di valutazione della sicurezza globale deve essere completato prima di avvalersi dell'opera di terzi che hanno accesso alle reti o ai dati elettronici sensibili di Stryker o che forniscono soluzioni basate su internet o software per l'uso interno o l'utilizzo su di un prodotto o sull'offerta di servizi da parte di Stryker.

4. **Uso delle apparecchiature e dei sistemi Stryker:** Qualsiasi dipendente di Stryker o terza parte che abbia accesso alle apparecchiature o ai sistemi di Stryker userà i suddetti strumenti in maniera conforme ai requisiti applicabili per un uso accettabile.

Responsabilità

È responsabilità di tutti i dipendenti Stryker e dei terzi attenersi alle indicazioni della presente politica e a tutte le norme e procedure di implementazione applicabili. Il CISO, in coordinamento con tutte le altre funzioni pertinenti e le unità aziendali, deve identificare quali siano le norme e le procedure aggiuntive necessarie per la conformità a questa Politica e deve preparare ed implementare tali norme e procedure.

Conformità

Stryker richiede a tutti i dipendenti e terzi di attenersi alle indicazioni della presente Politica. In caso di domande su questa politica o sulle procedure attinenti o di problemi relativi al programma di sicurezza di Stryker, si prega di contattare il rappresentante locale delle Risorse umane, il Compliance Officer, un consulente legale o l'hotline Etica. Stryker tratterà tali segnalazioni come informazioni riservate in conformità alle politiche e alle procedure dell'hotline.