Politica corporativă 7

Securitatea globală a informațiilor și sistemelor

Scop

Scopul acestei Politici este de a stabili angajamentul Stryker de aplicare a unor măsuri de control de securitate adecvate în cadrul informațiilor, sistemelor și operațiunilor sale, în concordanță cu legislația aplicabilă.

Domeniul de aplicare

Prezenta Politică se aplică tuturor angajaților Stryker și terților (de ex. furnizori, contractanți, mandatari) care acționează în numele Stryker, indiferent de locație. Dacă orice prevedere a prezentei Politici nu este conformă legislației locale sau regionale aplicabile unei anumite entități juridice Stryker, entitatea respectivă, în măsura necesară, va implementa o anexă la prezenta Politică, pentru a respecta legislația locală sau regională, cu condiția ca politica revizuită să respecte în cea mai mare măsură posibilă principiile incluse în prezenta Politică. O astfel de anexă va fi aprobată de CISO. În cazul în care nu a fost implementată o anexă locală sau regională, toate prevederile prezentei Politici rămân în vigoare în măsura în care sunt conforme cu legislația aplicabilă.

Politicile de bază

Stryker va respecta toate legile care reglementează securitatea produselor și sistemelor Stryker. În plus, Stryker își exprimă angajamentul pentru standardele stabilite mai jos.

1. **Numirea unui responsabil șef cu securitatea informațiilor (CISO):** CISO este responsabil pentru stabilirea și implementarea funcționării eficiente a programului global de securitate a informațiilor al Stryker și alinierea inițiativelor de securitate cu programele și obiectivele de afaceri ale societății, și pentru protejarea activelor, produselor, sistemelor și tehnologiilor.

2. **Implementarea politicilor de securitate și a structurilor administrative și de guvernanță:** Stryker, prin intermediul Sistemelor de management al calității aplicabile, al Sistemului de management al securității informațiilor, al standardelor de guvernanță a informațiilor, al standardelor privind Utilizarea acceptabilă, al Planului de răspuns în caz de incident și al procedurilor și standardelor aferente, va implementa măsurile de control administrative, tehnice și fizice de securitate.

3. **Evaluarea terților:** Procesul global de evaluare a securității trebuie finalizat înainte de angajarea oricărui terț care are acces la rețelele Stryker sau la datele electronice cu caracter sensibil, sau furnizează soluții pe bază de internet, sau software pentru uz intern sau utilizare în cadrul ofertei de produse sau servicii Stryker.

4. **Utilizarea echipamentelor și sistemelor Stryker:** Orice angajat al Stryker sau terț, care are acces la echipamentele sau sistemele Stryker, va utiliza respectivele echipamente și sisteme în conformitate cu cerințele aplicabile privind utilizarea acceptabilă.

Responsabilități

Este în responsabilitatea tuturor angajaților Stryker și a terților să respecte prezenta Politică și toate standardele și procedurile de implementare aplicabile. CISO, împreună cu alte funcții și unități de afaceri adecvate, va identifica orice standarde și proceduri suplimentare necesare pentru respectarea prezentei Politici și va elabora și implementa respectivele standarde și proceduri.

Conformitate

Stryker solicită tuturor angajaților și terților să respecte prezenta Politică. Dacă aveți o întrebare cu privire la prezenta Politică sau procedurile aferente sau dacă aveți o preocupare cu privire la programul de securitate al Stryker, vă rugăm să contactați reprezentantul local al Departamentului de resurse umane al Stryker, un responsabil pentru conformitate, consilierul juridic sau Linia de asistență pentru etică. Stryker va păstra astfel de raportări în condiții de confidențialitate, în conformitate cu politicile și procedurile Liniei de asistență.