Politique d'entreprise 7

Sécurité des systèmes et des renseignements généraux

But

Le but de la présente politique est d'énoncer l'engagement de Stryker de mettre en place des contrôles de sécurité appropriés dans le cadre de ses renseignements, systèmes et activités, conformément au droit applicable.

Portée

Cette politique concerne tous les employés de Stryker et les tiers (par ex., vendeurs, entrepreneurs, agents) agissant pour le compte de Stryker, quel que soit son emplacement. Si une disposition de la présente politique n'est pas conforme à la législation locale ou régionale applicable à une entité juridique spécifique de Stryker, cette entité doit, dans la mesure nécessaire, ajouter une annexe à la présente politique pour se conformer à la législation locale ou régionale, à condition que la politique révisée soit dans la mesure du possible conforme aux principes contenus dans cette politique. Une pareille annexe doit être approuvée par le RSSI. Lorsqu'une annexe locale ou régionale a été mise en place, toutes les dispositions de cette Politique demeureront en vigueur dans la mesure où elles respectent les règles de droit applicables.

Politiques de base

Stryker se conformera à l'ensemble des lois réglementant la sécurité des produits et systèmes de Stryker. De plus, Stryker est déterminée à respecter les normes établies ci-dessous.

1. **Nommer un responsable de la sécurité des systèmes d'information (RSSI) :** Le RSSI est chargé de la mise en place et de l'application efficaces du programme de sécurité générale de l'information de Stryker et de l'alignement des initiatives de sécurité sur les programmes et les objectifs de l'entreprise en matière de protection des actifs, produits, systèmes et technologies.

2. **Mettre en œuvre des politiques de sécurité ainsi que des structures administratives et de gouvernance :** Stryker mettra en pratique, par le biais de systèmes de gestion de la qualité, du système de gestion de la sécurité de l'information, des normes de gouvernance de renseignements, des normes d'utilisation acceptable, du plan de réponse aux incidents et des normes et procédures associées, les contrôles de sécurité administratifs, techniques et physiques appropriés.

3. **Évaluation de tierces parties :** Le processus d'évaluation de la sécurité générale doit être terminé avant de faire appel à une tierce partie ayant accès aux réseaux ou aux données sensibles électroniques de Stryker ou aux solutions ou logiciels Internet à utiliser à des fins internes ou dans une offre de produits ou de services Stryker.

4. **Utilisation de l'équipement et des systèmes de Stryker :** Tout employé de Stryker ou toute tierce partie ayant accès à l'équipement ou aux systèmes de Stryker l'utilisera conformément aux exigences applicables en matière d'utilisation acceptable.

Responsabilités

Il est de la responsabilité de tous les employés de Stryker et des tierces parties de se conformer à la présente politique ainsi qu'à toutes les normes et procédures de mise en œuvre applicables. Le RSSI, en collaboration avec d'autres fonctions et unités fonctionnelles, répertorie toutes les normes et procédures supplémentaires nécessaires au respect de la présente politique et prépare et met en place ces normes et procédures.

Conformité

Stryker exige que tous les employés et tierces parties se conforment à la présente politique. Si vous avez des questions à propos de la présente politique, des procédures connexes ou du programme de sécurité de Stryker, veuillez contacter le représentant local des ressources humaines de Stryker, un responsable de la conformité, un conseiller juridique ou la ligne d'assistance en matière d'éthique. Stryker préservera la confidentialité de ces rapports conformément aux politiques et procédures de la ligne d'assistance.