Politique d'entreprise n° 7

Sécurité globale de l'information et des systèmes

Objectif

Le but de cette politique est d'énoncer l'engagement de Stryker à mettre en place des contrôles de sécurité appropriés en matière d'information, de systèmes et d'opérations, conformément aux lois en vigueur.

Champ d'application

Cette politique s'applique à tous les employés de Stryker et aux tiers (vendeurs, sous-traitants, agents, par exemple) agissant pour le compte de Stryker, quel que soit le lieu. 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, mettre en place 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. Cette annexe doit être approuvée par le RSSI (responsable de la sécurité de l'information). Si une annexe locale ou régionale n'a pas été mise en place, toutes les dispositions de la présente politique resteront en vigueur dans la mesure où elles sont conformes à la loi applicable.

Politiques fondamentales

Stryker se conformera à toutes les lois régissant la sécurité des produits et des systèmes de Stryker. En outre, Stryker s'engage à respecter les normes énoncées ci-après.

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

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

3. **Évaluer les tiers :** Le processus d'évaluation de la sécurité globale doit être terminé avant d'engager un tiers ayant accès aux réseaux ou aux données sensibles électroniques de Stryker ou fournissant des solutions ou des logiciels basés sur Internet, à utiliser en interne ou dans le cadre d'une offre de produits ou de services Stryker.

4. **Utilisation des équipements et des systèmes Stryker :** Tout employé de Stryker ou tout tiers ayant accès à l'équipement ou aux systèmes de Stryker les utilisera conformément aux exigences d'utilisation acceptables applicables.

Responsabilités

Il est de la responsabilité de tous les employés de Stryker et des tiers de se conformer à la présente politique ainsi qu'à toutes les normes et procédures de mise en œuvre applicables. Le RSSI, conjointement avec les autres fonctions et unités opérationnelles concernées, doit identifier toutes les normes et procédures supplémentaires nécessaires au respect de la présente politique et préparer et mettre en œuvre ces normes et procédures.

Conformité

Stryker exige de tous les employés et tiers qu'ils se conforment à cette politique. Si vous avez des questions sur la présente politique ou sur les procédures associées, ou si vous avez des préoccupations concernant le programme de sécurité de Stryker, veuillez contacter le représentant local des ressources humaines de Stryker, un responsable de la conformité, un conseiller juridique ou le service d'assistance en matière d'éthique. Stryker préservera la confidentialité de ces rapports conformément aux politiques et procédures du service d'assistance.