Корпоративная политика № 7

Глобальная безопасность информации и систем

Цель

Цель настоящей Политики — заявить о приверженности компании Stryker соответствующим мерам безопасности в отношении ее информации, систем и деятельности в соответствии с действующим законодательством.

Сфера применения

Настоящая Политика применяется ко всем сотрудникам компании Stryker и третьим лицам (например, поставщикам, подрядчикам, агентам), действующим от имени компании Stryker, независимо от их местонахождения. Если какое-либо положение настоящей Политики не соответствует местному или региональному законодательству, применимому к конкретному юридическому лицу компании Stryker, эта организация должна (если необходимо) разработать приложение к настоящей Политике в соответствии с местным или региональным законодательством при условии, что пересмотренная политика будет в максимально возможной степени соответствовать принципам, изложенным в настоящей Политике. Такое приложение должно быть одобрено директором по информационной безопасности. Если местное или региональное приложение разработано не было, все положения настоящей Политики остаются в силе, если это соответствует применимому законодательству.

Основные политики

Компания Stryker соблюдает все законы, регулирующие безопасность продуктов и систем компании Stryker. Кроме того, компания Stryker придерживается изложенных ниже стандартов.

1. **Назначение директора по информационной безопасности (ДИБ):** ДИБ отвечает за создание и обеспечение эффективного соблюдения общей программы информационной безопасности компании Stryker, а также засогласование инициатив по обеспечению безопасности с корпоративными программами и целями компании по защите информационных активов, продуктов, систем и технологий.

2. **Реализация политики по безопасности и административных и управленческих структур:** Компания Stryker будет осуществлять соответствующие административные, технические и физические меры безопасности с помощью соответствующих систем управления качеством, системы управления информационной безопасностью, стандартов управления информацией, стандартов допустимого использования, плана реагирования на инциденты и соответствующих стандартов и процедур.

3. **Оценка третьих лиц:** До привлечения любого третьего лица, которое имеет доступ к сетям или электронным конфиденциальным данным компании Stryker или предоставляет онлайн-решения или программное обеспечение для внутреннего использования или использования в продукте или предложении компании Stryker, должен быть выполнен процесс общей оценки безопасности.

4. **Использование оборудования и систем компании Stryker:** Любой сотрудник компании Stryker или третье лицо, имеющее доступ к оборудованию или системам компании Stryker, обязаны использовать это оборудование и системы в соответствии с применимыми требованиями допустимого использования.

Обязанности

Все сотрудники компании Stryker и третьи лица несут ответственность за соблюдение настоящей Политики и всех применимых стандартов и процедур. ДИБ совместно с соответствующими отделами и подразделениями будет определять дополнительные стандарты и процедуры, необходимые для соблюдения настоящей Политики, с последующими подготовкой и внедрением таких стандартов и процедур.

Соблюдение требований

Компания Stryker требует соблюдения настоящей Политики от всех сотрудников и третьих лиц. Если у вас есть вопросы об этой Политике или связанных с ней процедурах, или если у вас есть сомнения относительно программы безопасности компании Stryker, свяжитесь с местным представителем компании Stryker по работе с персоналом, комплаенс офицером, сотрудником юридического департамента, или обратитесь на горячую линию по вопросам этики. Компания Stryker обязуется сохранять конфиденциальность сообщений в соответствии с правилами и процедурами горячей линии.