Протокол безопасности

Информационная безопасность имеет для нас решающее значение. Политика Международного Центра LA STRADA заключается в том, чтобы приложить все усилия для защиты информации от угроз - внутренних или внешних, преднамеренных или случайных. В своей работе мы руководствуемся следующими принципами:

- Конфиденциальность - предотвращение несанкционированного раскрытия информации;
- Целостность - предотвращение несанкционированного изменения информации;
- Доступность - установление соответствующих уровней доступа и безопасности для предотвращения несанкционированного доступа и поддержания законного доступа.

Наша приверженность информационной безопасности подтверждается внедрением процедур управления информационной безопасностью. Эти процедуры включают требования и правила по защите всей информации, включая персональные данные.

Безопасность и защита данных в информационной системе Службы сообщений реализуется с помощью следующих мер:

1.Общие меры управления информационной безопасностью:

- обеспечена безопасность и физический доступ к средствам представления информации с целью предотвращения ее просмотра посторонними лицами (экран компьютера не виден снаружи и не может быть виден другим сотрудникам организации; окно закрыто защитной матовой пленкой или жалюзи);
- все программное обеспечение, используемое в ИТ-системе, соответствует условиям лицензирования. Установка программного обеспечения осуществляется администратором информационной системы;
- установка антивирусных приложений для защиты данных от кибератак, вредоносного ПО или кражи персональных данных.

2.Безопасность физической среды и информационных технологий, используемых в процессе обработки информации

- Доступ в офис Службы сообщений, где расположены информационные системы персональных данных, ограничен и разрешен только лицам, имеющим необходимые полномочия (аналитикам, координаторам),
- Доступ в блок через главный вход защищен навесным замком и системой чип-карт. Вход посторонних в блок невозможен без разрешения сотрудника организации. Вход в офис службы невозможен, доступ имеют только уполномоченные лица, дверь постоянно заперта, наличие входных табличек запрещено.
- Периметр здания или помещений, в которых находится оборудование для обработки информации, физически цел, внешние стены помещений прочные, входы оборудованы замками и сигнализацией.
- Расположение средств обработки информации соответствует необходимости обеспечения их безопасности от несанкционированного доступа, кражи, пожара, затопления и других возможных рисков.

- Компьютеры, серверы, другие терминалы доступа располагаются в местах с ограниченным доступом посторонних лиц.
- Использование фото-, видео-, аудио- и иной записывающей аппаратуры в офисе Службы допускается только с особого разрешения руководства.

3.Аутентификация пользователей и защита доступа

- Осуществляется идентификация и аутентификация пользователей информационных систем Службы и процессов, выполняемых от имени этих пользователей.
- Все пользователи (аналитики, Координатор Службы, в том числе Администратор сети) имеют персональный идентификатор (User ID), который соответствует уровню доступности пользователя.
- Для подтверждения идентификатора пользователя используются пароли, специальные физические средства доступа с помощью карт памяти или микропроцессоров, биометрические средства аутентификации, основанные на уникальных и индивидуальных характеристиках человека.

Новые сотрудники Службы сообщений проходят обучение по вопросам информационной безопасности во время вступительного периода, и все сотрудники обязаны регулярно посещать курсы повышения квалификации, чтобы обеспечить актуальность своих знаний.

У нас есть отдельный информационный бюллетень о конфиденциальности, в котором разъясняются конкретные меры по обработке персональных данных. Его можно найти на нашем сайте www.siguronline.md.

Соблюдение политики и процедур информационной безопасности - это наша общая ответственность, к которой мы все относимся со всей серьезностью.