

Техническая безопасность

1. Общие положения

1.1. Настоящая Политика технической безопасности компании «InfraTech» (далее — Политика) определяет основные меры защиты данных и обеспечения безопасного функционирования сайта «infratech.kz» (далее — Сайт).

1.2. Политика направлена на предотвращение несанкционированного доступа, утечек данных и других угроз, которые могут повлиять на работу Сайта и защиту информации Пользователей.

1.3. Компания имеет право вносить изменения в настоящую Политику, публикуя актуальную версию на Сайте.

1.4. Пользователи обязаны самостоятельно отслеживать изменения в Политике.

1.5. Используя Сайт, Пользователь подтверждает, что принимает условия настоящей Политики в полном объеме. В случае несогласия с любыми положениями, Пользователь должен прекратить использование Сайта.

2. Защита данных и технологий

2.1. Компания применяет современные методы защиты данных, включая:

Шифрование данных при передаче и хранении с использованием SSL/TLS.

Шифрование данных при передаче и хранении с использованием SSL/TLS.

Регулярное обновление программного обеспечения и систем защиты.

Регулярное обновление программного обеспечения и систем защиты.

Мониторинг и анализ подозрительной активности для предотвращения угроз.

Мониторинг и анализ подозрительной активности для предотвращения угроз.

2.2. Доступ к данным ограничивается только уполномоченными сотрудниками компании.

2.3. Мы используем многоуровневые системы защиты, такие как брандмауэры, антивирусы и системы предотвращения вторжений (IDS/IPS).

3. Управление доступом

3.1. Компания внедрила многофакторную аутентификацию (MFA) для защиты учетных записей пользователей.

3.2. Каждому пользователю предоставляются уникальные учетные данные, которые защищены шифрованием.

3.3. Неавторизованный доступ к данным или системам блокируется автоматически.

4. Резервное копирование и восстановление

4.1. Регулярное резервное копирование данных выполняется для предотвращения их утраты.

4.2. Резервные копии хранятся в защищенных зонах, недоступных для несанкционированного доступа.

4.3. Механизмы восстановления данных позволяют минимизировать время простоя системы в случае непредвиденных ситуаций.

5. Обнаружение и устранение уязвимостей

5.1. Компания проводит регулярные аудиты безопасности для выявления потенциальных уязвимостей.

5.2. Мы сотрудничаем с профессиональными организациями для тестирования защиты данных (например, через программы тестирования на проникновение — pentesting).

5.3. В случае обнаружения угрозы компания немедленно принимает меры для её устранения.

6. Ответственность за безопасность

6.1. Мы придерживаемся международных стандартов безопасности, включая ISO/IEC 27001, PCI DSS и другие.

6.2. Компания регулярно обучает своих сотрудников вопросам информационной безопасности.

7. Сообщение о проблемах безопасности

7.1. Если вы обнаружили уязвимость на нашем Сайте или подозреваете угрозу, свяжитесь с нами по электронной почте: info@infratech.kz.

7.2. Все сообщения о проблемах безопасности рассматриваются оперативно, а необходимые меры принимаются в кратчайшие сроки.

8. Изменения в Политике

8.1. Политика технической безопасности может обновляться для соответствия новым стандартам и требованиям.

8.2. Обновленная версия Политики публикуется на Сайте и вступает в силу с момента её публикации.

9. Контактная информация

9.1. Для вопросов по технической безопасности обращайтесь по адресу: info@infratech.kz.

Наша главная цель — обеспечить безопасное и надежное использование Сайта для всех пользователей.