Информационная безопасность и защита данных

Мы стремимся поддерживать стабильность и надежность среди своих портфельных компаний и прикладываем все усилия для защиты персональных данных наших работников и клиентов от утечки, кражи или потери.

В Фонде организован Комитет по информационной безопасности, который дает рекомендации по вопросам обеспечения информационной безопасности в портфельных компаниях, а также поддерживает постоянное взаимодействие с государственными органами и с другими заинтересованными сторонами для лучшего решения вопросов безопасности в информационном пространстве.

Мы внедрили «Основные правила политики информационной безопасности» с приложениями в виде методик, руководств и правил, которые производят охват требуемой деятельности информационной безопасности и специалистов информационных технологий, а также всех сотрудников в части исполнения мер для обеспечения информационной безопасности. GRI 3-3

Мы проводим работу по разработке Корпоративного стандарта информационной безопасности, регулирующий общий свод правил по обеспечению информационной безопасность и управление процессом координации деятельности в группе компаний Фонда. Имеются процедуры по обеспечению информационной безопасности, решению инцидентов информационной безопасности, управлению доступом пользователей в информационные системы и другие. GRI 3-3

Ежегодно формируется регистр рисков по кибербезопасности и ежеквартально отчет по рискам, в том числе касательно группы компании Фонда.

В 2023 году проведены аудиты портфельных компаний Фонда на исполнение требований информационной безопасности, выработаны рекомендации по приведению в соответствие и повышений уровня информационной безопасности. GRI 3-3

Наши принципы для минимизации рисков в информационной безопасности:

- быстрое выявление, анализ и прогноз развития угроз в информационных технологиях, способных негативно повлиять на стабильность и надежность работы Фонда;
- оценка влияния неблагоприятных факторов;
- приоритетность требований по информационной безопасности;
- непрерывность обеспечения информационной безопасности;
- контролируемость и эффективность мер.

Инициированы мероприятия по внедрению международного стандарта по информационной безопасности ISO 27001 в Фонде. Создана рабочая группа для принятия участия в формировании реестра информационных активов и проведения классификации активов по степеням значимости.

А также, в рамках соблюдения кибергигиены для пользователей с помощью специализированного программного обеспечения проводится обучение и тестирование сотрудников Фонда.

На базе созданного Мониторингового центра для сопровождения систем информационной безопасности от внешних и внутренних угроз ИТ-инфраструктуры в условиях Фонда и оперативного центра информационной безопасности ТОО «QazCloud» обеспечиваем защиту данных. Компании в Группе Фонда продолжают усовершенствование системы информационной безопасности. В рамках взаимодействия рассматривались вопросы политик, проекты по повышению уровня и обеспечения информационной безопасности в портфельных компаниях.

Обеспечение безопасности информационных систем становится все более важным в условиях цифровой трансформации и роста угроз кибербезопасности. Наши усилия, в частности, направлены на защиту конфиденциальности данных клиентов.

Общее количество инцидентов, связанных с информационной безопасностью, составило 16 094 случая в отчетном году, в том числе 49% случаев приходится на обнаружение вредоносного программного обеспечения и несанкционированный доступ/взлом. Все инциденты своевременно отрабатываются, позволяя не допускать утечку данных клиентов. Инцидентов, связанных с данными клиентов не было.