Политика информационной безопасности

Руководство АО «ТЦ «ИНЖЕНЕР» (далее – Компания) осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития бизнеса и норм регулирования деятельности по защите информации, а также в контексте ожиданий клиентов.
Соблюдение требований по информационной безопасности, включая требования по обеспечению конфиденциальности данных клиентов, позволит создать конкурентные преимущества Компании, обеспечить её стабильность, соответствие правовым, регуляторным и договорным требованиям и повышение имиджа.
Для эффективной реализации процессов обеспечения информационной безопасности и защиты персональных данных в Компании внедрены развитые процессы обеспечения информационной безопасности.

1. Цели и задачи

Целью обеспечения информационной безопасности является поддержание устойчивого функционирования и развитие услуг Компании, защита процессов и активов, принадлежащих Компании и её клиентам.
Цели Компании в области информационной безопасности:

- устойчивое функционирование и развитие Компании, обеспечение непрерывности предоставления услуг клиентам;
- поддержание статуса Компании как надежного поставщика услуг по информационной безопасности в глазах действующих и потенциальных клиентов, увеличение инвестиционной привлекательности;
- гарантия защищенности процессов и активов, принадлежащих Компании и её клиентам;
- соблюдение законодательных и иных регуляторных требований в области информационной безопасности.

Задачи, решаемые для достижения целей в области информационной безопасности:

- отслеживание, анализ и внедрение применимых требований законодательства, национальных стандартов и регулирующих документов в области информационной безопасности;
- управление рисками информационной безопасности;
- применение организационных и технических мер по обеспечению информационной безопасности, использование передовых технологий противодействия угрозам информационной безопасности;
- применение лучших практик и принципов безопасной разработки программного обеспечения;
- вовлечение работников Компании в процессы обеспечения информационной безопасности, повышение уровня ответственности, осведомленности, постоянное обучение и получение обратной связи;
- обеспечение непрерывности бизнеса на основе комплекса организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов, а также направленных на бесперебойное оказание услуг Клиентам;
- регулярная оценка соответствия системы обеспечения информационной безопасности применимым внутренним и внешним требованиям посредством проведения внутренних аудитов, мониторинга эффективности процессов.

2. Принципы управления информационной безопасностью

Компания в области информационной безопасности руководствуется следующими основными принципами:

- *Законность*. Защита активов Компании соответствует положениям и требованиям действующих международных и национальных законов, и иных нормативных правовых актов.

- *Системность*. Системный подход к обеспечению требований информационной безопасности означает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения задачи защиты информации и персональных данных.
- *Комплексность*. Информационная безопасность обеспечивается эффективным сочетанием организационных и методических мер, а также программно-технических средств. Применение различных средств и технологий защиты процессов и активов снижает вероятность реализации наиболее значимых угроз информационной безопасности.
- *Непрерывность совершенствования*. Меры и средства защиты активов, как и система обеспечения информационной безопасности, постоянно совершенствуются, учитывается появление новых способов и средств реализации угроз информационной безопасности, а также принимается во внимание имеющийся опыт других организаций в сфере информационной безопасности.
- *Разумная достаточность и адекватность*. Программно-технические средства и организационные меры, направленные на защиту активов, проектируются и внедряются на основе регулярной оценки рисков таким образом, чтобы не повлечь за собой существенное ухудшение основных функциональных характеристик, а также производительности информационных систем Компании.
- *Персональная ответственность*. Ответственность за соблюдение требований информационной безопасности возлагается на каждого работника в пределах его полномочий.
- *Контроль*. С целью своевременного выявления и пресечения попыток нарушения установленных правил в Компании определены процедуры постоянного контроля функционирования системы обеспечения информационной безопасности, а результаты контроля подвергаются регулярному анализу.

Руководство Компании личным примером демонстрирует свое лидерство, придерживаясь требований информационной безопасности самостоятельно, а также способствуя вовлечению и активному участию персонала Компании в процессах обеспечения информационной безопасности.

Руководство Компании берет на себя ответственность за соответствие положений политики информационной безопасности требованиям заинтересованных сторон, назначение ответственных за решение соответствующих задач для достижения этих целей на всех уровнях, за их реализацию, периодический анализ и пересмотр, а также за непрерывное улучшение процессов информационной безопасности.

Положения настоящей Политики информационной безопасности являются обязательными для исполнения работниками всех структурных подразделений Компании, а также работниками подрядных организаций, если это предусмотрено договором.