meriterra.ru

meriterra

603089, Нижний Новгород, Сергиевская, 21

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ/

Руководство ООО «Меритерра» (далее – Компания) осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития российского и международного законодательства и норм регулирования деятельности по защите информации и персональных данных, а также в контексте ожиданий заинтересованных сторон.

Соблюдение требований по информационной безопасности позволит создать конкурентные преимущества Компании, обеспечить её стабильность, соответствие правовым, регуляторным и договорным требованиям и повышение имиджа.

Для эффективной реализации процессов обеспечения информационной безопасности в Компании внедрена система менеджмента информационной безопасности (далее – СМИБ) в соответствии с требованиями международного стандарта ISO/IEC 27001:2013.

1. Цели и задачи

Целью обеспечения информационной безопасности является поддержание устойчивого функционирования 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 разработке программного обеспечения и поддержке и администрированию инфраструктуры клиентов;
- гарантия защищенности процессов и активов, принадлежащих Компании и её клиентам;
- соблюдение законодательных и иных регуляторных требований законодательства Российской Федерации в области информационной безопасности и защиты персональных данных.

Задачи, решаемые для достижения целей в области информационной безопасности:

- обеспечение выполнения требований законодательства Российской Федерации в области защиты информации и персональных данных, а также национальных стандартов и регулирующих документов в области информационной безопасности;
- управление рисками информационной безопасности;
- применение различных организационных и технических мер по обеспечению информационной безопасности, использование передовых технологий противодействия угрозам информационной безопасности;
- вовлечение работников Компании в процессы обеспечения ИБ, 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 СМИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов, мониторинга эффективности процессов СМИБ, анализа со стороны руководства Компании;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СМИБ внутренним и внешним требованиям.

2. Принципы управления информационной безопасностью

Компания в области информационной безопасности руководствуется следующими основными принципами.

- *Законность*. Защита активов Компании соответствует положениям и требованиям международных и национальных действующих 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, методических мер и 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 постоянно совершенствуются в соответствии с результатами анализа функционирования системы менеджмента информационной безопасности, 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 обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.
- *Контроль*. Оценка эффективности системы защиты информации является неотъемлемой частью работ по обеспечению информационной безопасности. С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности активов в Компании определены процедуры постоянного контроля использования систем обработки и защиты активов, а результаты контроля подвергаются регулярному анализу.

Руководство Компании личным примером демонстрирует свое лидерство и приверженность в отношении СМИБ и способствует 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, доведение и разъяснение их работникам Компании и заинтересованным сторонам, 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 СМИБ.

Положения настоящей Политики информационной безопасности являются обязательными для исполнения работниками всех структурных подразделений Компании.