1. Назначение и область действия

1.1. «Политика информационной безопасности» (далее - Политика) демонстрирует позицию и намерения руководства ООО «Системный интегратор» (далее также – Общество) в области информационной безопасности, определяет основные цели и принципы ее обеспечения, устанавливает роли и ответственность исполнителей.

1.2.Под информационными активами Общество понимает информацию во всех ее формах и на всех стадиях жизненного цикла, связанные с ней информационную инфраструктуру и информационные процессы.

1.3.Политика предназначена для изучения и неукоснительного исполнения руководителями и работниками всех структурных подразделений Общества, подлежит доведению до сведения клиентов, партнеров и других заинтересованных сторон.

2. Положения политики

2.1. Под своей информационной безопасностью ООО «Системный интегратор» понимает защищенность бизнеса от угроз информационным активам, принадлежащим Обществу или находящимся в его распоряжении, а ее исключительная важность предопределена прямой зависимостью бизнеса от репутации надежного и эффективного поставщика ИТ-услуг.

2.2. Важнейшими целями совершенствования управления информационной безопасностью Общество видит:

- предоставление нашим клиентам информационно-технологических услуг, качество которых отвечает лучшим мировым стандартам и в полной мере способствует удовлетворению их потребностей в обеспечении благоприятных условий для стабильного существования и динамичного роста;
- сохранение и развитие своего конкурентного преимущества и доверия наших клиентов за счет применения передовых технологий и методов управления информационными рисками, минимизирующих негативное влияние угроз в информационной сфере на реализацию бизнес-целей;
- недопущение нанесения интересам государства, общества, наших клиентов, партнеров и работников неприемлемого ущерба, могущего повлечь отрицательные последствия для нашего устойчивого функционирования.

2.3. Основными приоритетами ООО «Системный интегратор» в достижении заявленных целей являются:

- обеспечение конфиденциальности, целостности и доступности информационных ресурсов, соизмеряемое с требованиями и рисками бизнеса;
- организация системы управления информационной безопасностью как непрерывного циклического процесса, включающего планирование, реализацию, оценку и улучшение защитных мер;
- инвентаризация и классификация информационных активов по их ценности для Общества, закрепление ответственности за информационные активы и контроль доступа к ним;
- использование документированных и экономически обоснованных мер защиты, адекватных опасности угроз и вероятности их проявления;
- осуществление деятельности по управлению информационной безопасностью как неотъемлемой части общей деятельности по обеспечению непрерывности бизнеса;
- соблюдение требований действующего законодательства, применимых международных, отраслевых и корпоративных стандартов, принятых на себя договорных обязательств, а также законных прав наших работников, клиентов и партнеров;
- выявление и анализ несоответствий существующей практики обеспечения информационной безопасности установленным требованиям, определение упреждающих и корректирующих мер и контроль их эффективности.

3. Роли и ответственность

3.1. Руководство Общества принимает на себя личную ответственность за:

- принятие решений, определяющих политику в области информационной безопасности, планов по управлению рисками, действий по постоянному улучшению информационной безопасности;
- поддержку деятельности по обеспечению информационной безопасности необходимыми организационными, финансовыми и людскими ресурсами.

3.2. На руководителей структурных подразделений Общества руководство возлагает:

- организацию повседневной деятельности по обеспечению информационной безопасности как неотъемлемой составляющей производственных процессов;
- своевременную идентификацию значимых информационных активов, назначение ответственных за них и контроль доступа;
- предъявление установленных Обществом требований информационной безопасности к работникам, клиентам и партнерам, использующим его информационные активы, и контроль за их выполнением.

3.3. На руководителя структурного подразделения информационной безопасности руководство возлагает:

- создание, внедрение и совершенствование нормативной и методической базы Общества по обеспечению информационной безопасности;
- сбор и представление свидетельств, позволяющих оценить эффективность применяемых мер, их соответствие политике информационной безопасности, а также спланировать действия по улучшению.

3.4. На руководителей подразделений поддержки информационных систем и технической инфраструктуры руководство возлагает разработку внедрение и сопровождение технических средств, поддерживающих выполнение политик и процедур в области информационной безопасности.

3.5. Руководство Общества ожидает от работников ООО «Системный интегратор», а также клиентов и партнеров, использующих его информационные активы:

- понимания и выполнения его политики в области информационной безопасности;
- информирования обо всех событиях, способных помочь сохранению и улучшению информационной безопасности Общества.

3.6. Дополнительные поручения Руководства изложены им в политиках информационной безопасности по соответствующим предметным областям.

3.7. Нарушения информационной безопасности Общества могут служить основанием для привлечения к ответственности, предусмотренной законодательством или соглашением сторон.

3.8. Контроль за выполнением Политики и ее пересмотр на регулярной основе, а также по результатам анализа деятельности, при изменениях организационной и технологической структуры, стоимости и эффективности защитных мер, иных событиях, значимых для оценки рисков, осуществляется Руководством.