Товарищество с ограниченной ответственностью “ IoT Solutions”

УТВЕРЖДЕНО

Директор ТОО “IoT Solutions”

_____ Баев Владимир Викторович

«30» апреля 2024 г.

М. П.

Политика информационной безопасности ТОО «IoT Solutions»

1. Общие положения

Настоящая Политика является основополагающим документом в области информационной безопасности и служит руководством при разработке соответствующих Положений, Правил и Инструкций.

Область распространения Политики: обеспечение безопасности информационно-коммуникационной инфраструктуры в ТОО «IoT Solutions» (далее – компания) при реализации программного обеспечения и сервисов, при оказании услуг проектирования, разработки, внедрения, эксплуатации сервисов и/или программного обеспечения, хранению, накоплению и обработке персональных данных и иных решений в области информационных технологий применяется система менеджмента информационной безопасности.

Компания стремится соответствовать международным требованиям обеспечения информационной безопасности за счет поддержания в рабочем состоянии и развития системы менеджмента информационной безопасности согласно стандарту менеджмента информационной безопасности СТ РК ISO/IEC 27001-2022 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

2. Цели, задачи и принципы

2.1 Цели

Целью информационной безопасности Компании является:

1) обеспечение информационной безопасности при осуществлении деятельности компании;
2) защита конфиденциальной информации компании;
3) обеспечение соблюдения законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью.

2.2 Задачи

Для достижения поставленных целей необходимо решить следующие задачи:

a) защита от вмешательства посторонних лиц в процесс функционирования ЭИР компании;

b) разграничение доступа зарегистрированных пользователей к информации, аппаратным, программным и криптографическим средствам защиты, используемым в компании;

c) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

d) защита информации от несанкционированной модификации и искажения;

e) контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносных кодов, включая компьютерные вирусы;

f) обеспечение аутентификации пользователей компании;

g) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба.

2.3 Принципы

Построение системы обеспечения информационной безопасности компании и ее функционирование должны осуществляться в соответствии со следующими принципами:

1) законность – действия, направленные на обеспечение информационной безопасности, осуществляются на основе действующего законодательства;

2) ориентированность на бизнес – информационная безопасность рассматривается как процесс основной деятельности компании;

3) непрерывность – мероприятия по обеспечению информационной защиты компании должны осуществляться без прерывания текущих бизнес-процессов компании;

4) комплектность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

5) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам;

6) приоритетность – категорирование всех информационных ресурсов компании по степени важности при оценке реальных и потенциальных угроз информационной безопасности;

7) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными работниками;

9) принцип «чистого стола» в отношении бумажных документов и сменных информационных носителей и принцип «чистого экрана» в отношении электронных средств обработки информации;

10) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

11) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений компании, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями;

12) управление доступом – доступ к активам компании должен быть ограничен в соответствии с должностными обязанностями и актуализироваться в соответствии с результатами анализа рисков информационной безопасности. Предоставление привилегированных прав доступа должно строго ограничиваться и контролироваться;

13) криптографическая защита – криптографические механизмы могут использоваться в компании в следующих случаях: использования шифрования для обеспечения конфиденциальности информации при ее хранении или передаче и использование цифровых подписей для защиты аутентичности и целостности хранимой или передаваемой конфиденциальной информации. Криптографические средства должны использоваться в

соответствии с релевантными требованиями соглашений, законодательства и нормативных документов;

14) мобильные устройства и носители информации – мобильные устройства и носители информации должны использоваться только для выполнения должностных задач, за внесение несанкционированных изменений в настройки корпоративного мобильного устройства и в носители информации пользователь несет ответственность.

3. Ответственность и обязательства

Эффективная безопасность требует подотчетности, исчерпывающего определения и признания обязанностей в сфере безопасности. Руководство компании отвечает за все аспекты управления безопасностью, включая принятие решений по управлению рисками.

Руководство компании принимает непосредственное участие в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности компании (бизнеса), законами и нормативными актами.

За несоблюдение законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью, к работникам могут быть применены меры, предусмотренные соответствующими внутренними документами компании, трудовыми договорами и действующим законодательством Республики Казахстан.

Руководство компании обязано содействовать постоянному улучшению системы менеджмента информационной безопасности.

Ответственным лицом за контроль, реализацию, распространения, применения, исполнения, за развитие, оценку и пересмотр настоящего документа назначается сотрудник ответственный за обеспечение информационной безопасности.

Ответственный сотрудник за обеспечение информационной безопасности назначается приказом руководства Организации.

4. Пересмотр Политики информационной безопасности

Настоящий документ подвергается анализу и пересмотру не реже одного раза в два года или при возникновении существенных изменений, влияющих на соответствие требованиям стандартов, адекватности и эффективности применяемых мер обеспечения ИБ, выявленных в процессе внешнего или внутреннего аудита.

В ходе пересмотра следует оценить возможность улучшения положений политики информационной безопасности и процесса управления информационной безопасностью в соответствии с изменениями условий ведения бизнеса, законодательства, изменениями в организационной структуре, изменениями адекватной реальности и информационных угроз окружающей среды.

5. Документирование политики информационной безопасности

Настоящий документ, содержит политику информационной безопасности, утверждается руководством Организации и доводится до сведения всех сотрудников проекта, а также сторонних организаций и частных лиц в мере, соответствующей договорным и/или лицензионным отношениям и/или другим видам договоренностей с третьими лицами.

Утвержденные в Политике Нормативные ссылки **(Приложение 1)** и термины и определения **(Приложение 2)** распространяются на все соответствующие Положения, Правила и Инструкций по информационной безопасности.

Приложение 1

Нормативные ссылки

В настоящем документе используются материалы следующих документов:

1.1. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»;

1.2. Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите»;

1.3. Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи»;

1.4. Постановление Правительства Республики Казахстан от 12 ноября 2013 года № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач»;

1.5. Постановление Правительства Республики Казахстан от 3 сентября 2013 года № 909 «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных»;

1.6. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 5 июня 2019 года № 18795 «Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности»;

1.7. Приказ и. о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 февраля 2016 года № 13349 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации»;

1.8. Приказ Министра информации и коммуникаций Республики Казахстан от 13 июня 2018 года № 263. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 июня 2018 года № 17141 «Об утверждении Правил проведения аудита информационных систем»;

1.9. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (далее – ЕТ);

1.10. Приказ и. о. Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 13 апреля 2018 года № 16756 «Об утверждении Правил проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

1.11. СТ РК ISO/IEC 27000-2020 Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности Общий обзор и словарь;

1.12. СТ РК ISO/IEC 27001-2015 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования (далее – СТ РК ИСО/МЭК 27001-2015);

1.13. СТ РК ISO/IEC 27002-2015 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации (далее – СТ РК ИСО/МЭК 27002-2015);

1.14. СТ РК ISO/IEC 27003-2018 Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности Руководство;

1.15. СТ РК ISO/IEC 27005-2013 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности для связи между подразделениями и организациями;

1.16. СТ РК ISO/IEC 27010-2017 Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности при коммуникациях между секторами и между организациями;

1.17. СТ РК ISO/IEC 27031-2013 Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса;

1.18. СТ РК ISO/IEC 27035-1-2017 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности Часть 1 Принципы менеджмента инцидентов;

1.19. СТ РК ISO/IEC 27035-2-2017 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности Часть 2 Руководящие указания по планированию и разработке реагирования на инциденты;

1.20. СТ РК ИСО/МЭК 13335-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий;

1.21. СТ РК ИСО/МЭК 13335-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий;

1.22. СТ РК ИСО/МЭК 13335-4-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 4. Выбор защитных мер;

1.23. СТ РК ИСО/МЭК 13335-5-2008 Информационная технология Методы и средства обеспечения безопасности управление защитой информационных и коммуникационных технологий Часть 5 Руководство по управлению защитой сети;

1.24. СТ РК ИСО МЭК 31010-2010 Менеджмент риска. Методы оценки риска;

1.25. СТ РК ГОСТ Р 50739–2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

1.26. СТ РК 34.005–2002 Информационная технология. Основные термины и определения;

1.27. СТ РК 34.006–2002 Информационная технология. Базы данных. Основные термины и определения;

1.28. СТ РК 2190-2012 Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования;

1.29. СТ РК 2192-2012 Информационные технологии. Интернет-ресурс, интернет-портал, Интернет-портал. Общие описания;

1.30. СТ РК 2199-2012 Информационные технологии. Требования к безопасности Веб-приложений в государственных органах;

1.31. СТ РК 34.007–2002 Информационная технология. Телекоммуникационные сети. Основные термины и определения.

Приложение 2

Применяемые термины и сокращения

1.1. **Организация:** ТОО "**IoT Solutions**".

1.2. **Руководство Организации (Первый руководитель Организации; Руководитель Организации):** Директор ТОО " **IoT Solutions**".

1.3. **Ответственный сотрудник за обеспечение информационной безопасности (Ответственный сотрудник за обеспечение ИБ; Ответственный за обеспечение ИБ; СОИБ):** Сотрудник, отвечающий за контроль исполнения требований ИБ в Организации.

1.4. **Ответственный сотрудник по вопросам безопасности при работе с персоналом (СИБП):** Сотрудник, отвечающий за взаимодействие с ответственным за обеспечение ИБ, администраторами ИС, менеджером проекта и руководством Организации по вопросам безопасности при работе с персоналом.

1.5. **Операционные процедуры:** Действия, выполняемые персоналом в целях сопровождения, эксплуатации, обеспечения ИБ, технического обслуживания ИС, ЭИР.

1.6. **Политика (policy):** Намерения и направления, формально выраженные руководством [27002].

1.7. **Доступность (availability):** Свойство быть доступным и готовым к использованию по требованию авторизованного пользователя (сущности) [27001, ISO/IEC 13335-1].

1.8. **Интернет-ресурс (ИР)**: Электронный информационный ресурс, отображаемый в текстовом, графическом, аудиовизуальном или ином виде, размещаемый на аппаратно-программном комплексе, имеющий уникальный сетевой адрес и (или) доменное имя и функционирующий в Интернете [ЕТ].

1.9. **Конфиденциальность (confidentiality):** Свойство, что информация становится недоступной и не раскрывается для неавторизованных пользователей, сущностей или процессов. [27001, ISO/IEC 13335-1].

1.10. **Менеджер проекта (МП):** Сотрудник Организации, отвечающий за управление проектом разработки, развития, сопровождения и поддержки ИС и/или ЭИР, ответственный за обеспечение надлежащей работы информационной системы в процессе эксплуатации и сопровождения ИС и/или ЭИР.

1.11. **Мобильный код:** Программный код, который можно перенести с одного компьютера на другой, а затем запускать автоматически для выполнения конкретной функции практически без взаимодействия с пользователем.

1.12. **Проприетарное программное обеспечение:** программное обеспечение, являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободного ПО (наличия открытого программного кода недостаточно). Правообладатель проприетарного ПО сохраняет за собой монополию на его использование, копирование и модификацию, полностью или в существенных моментах. Обычно проприетарным называют любое несвободное ПО, включая полусвободное [Free Software Foundation (FSF)].

1.13. **Свободное программное обеспечение:** ПО удовлетворяющее следующим критериям [The Debian Free Software Guidelines (DFSG)]:

1) свободное распространение: лицензия не ограничивает распространение, каким бы то ни было лицам или организациям, не требует денежной компенсации;

2) исходные тексты: они должны присутствовать, и лицензия не должна ограничивать их распространение;

3) производные работы: лицензия должна разрешать создание и распространение производных работ от данного ПО на тех же условиях, как и оригинал;

4) целостность авторских исходных текстов: лицензия может запрещать распространение производных работ от исходных текстов, но в этом случае она должна разрешать свободное распространение патчей для исходного текста;

5) запрещается дискриминация людей или групп людей;

6) запрещается дискриминации по областям деятельности;

7) распространение лицензии: лицензия распространяется на любого, кто получил копию ПО;

8) лицензия не должна ограничивать другое ПО.

1.14. **Лицензионное программное обеспечение:** ПО, распространение, эксплуатация, использование, модификация, ребрендеринг и другие манипуляции контролируются и/или ограничиваются лицензионным соглашением.

1.15. **Администратор ИС (АИС, СА):** Ответственный сотрудник Организации или подрядной организации, назначенный выполнять работы по сопровождению ИС, и поддержанию среды эксплуатации ИС.

1.16. **Система менеджмента (управления) информационной безопасностью (СМИБ):** Часть общей системы управления Организацией, основанная на оценке бизнес-рисков и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности [27001].

1.17. **Сопровождение информационной системы:** Этап жизненного цикла информационной системы, на протяжении которого выполняются работы для обеспечения функционирования информационной системы, а также работы по изменению (модификации) ПО и документов информационной системы, вызванные возникшими проблемами или потребностями в модернизации или настройке.

1.18. **Целостность (integrity):** Свойство сохранения точности и полноты ресурсов. [27001, ISO/IEC 13335-1].

1.19. **Электронный информационный ресурс (ЭИР):** Информация, предоставленная в электронно-цифровой форме и содержащаяся на электронном носителе, Интернет-ресурсе и (или) в информационной системе [ET].

1.20. **Электронная цифровая подпись (ЭЦП):** Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания [ET].

1.21. **Эксплуатация информационной системы:** Этап жизненного цикла информационной системы, на протяжении которого информационная система используются в соответствии с её функциональным назначением и в соответствии с требованиями действующих документов Общества, а также осуществляются все необходимые действия по поддержке пользователей.

1.22. **ОС:** Операционная система.

1.23. **ПО:** Программное обеспечение.

1.24. **ППО:** Прикладное программное обеспечение.

1.25. **ПП РК:** Постановление Правительства Республики Казахстан;

1.26. **ПИС, IPR:** Права на интеллектуальную собственность.

1.27. **СПО:** Системное программное обеспечение.

1.28. **БД:** База данных.

1.29. **СУБД:** Система управления базами данных.

1.30. **СП:** Сервер приложений.

1.31. **СК:** Серверная комната.

1.32. **ВП:** Веб-портал.

1.33. **ДМ:** Дисковый массив.

1.34. **РК:** Республика Казахстан.

1.35. **СКУД:** система контроля и управления доступом;

1.36. **СХД:** Система хранения данных.

1.37. **СЭ:** Сетевой экран.

1.38. **СЗИ:** Средства защиты информации.

1.39. **НУЦ РК, НУЦ:** Национальный удостоверяющий центр Республики Казахстан.

1.40. **ЭЦП:** Электронно-цифровая подпись.

1.41. **RSA (аббревиатура от фамилий Rivest, Shamir и Adleman):** криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.