Утверждена
протоколом Общего собрания участников
ТОО «Қамқор Менеджмент»
от «29» декабря 2023 года,
№ КМ-1-29-12-23

Политика
информационной безопасности
ТОО «Қамқор Менеджмент»

Оглавление:

Раздел 1. Общие положения

Глава 1. Цель, область применения, пользователи

1. Настоящая Политика информационной безопасности товарищества с ограниченной ответственность «Камкор Менеджмент» (далее – «Политика» и «Товарищество», соответственно) определяет основные цели, принципы, подходы, решения по обеспечению информационной безопасности (далее – ИБ) в Товариществе и выражает отношение (подход) Товарищества к обеспечению защиты информации в рамках своей деятельности.
2. Настоящая Политика обязательна для исполнения всеми структурными подразделениями (далее – СП) Товарищества, а также доводится до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам (далее – ИС) и документам Товарищества в той части, которая непосредственно связана с Товариществом и его деятельностью.
3. Пользователями настоящей Политики являются все работники Товарищества.
4. Ознакомление с настоящей Политикой является обязательным для каждого работника Товарищества при приеме на работу.

Глава 2. Нормативные ссылки

5. Настоящая Политика разработана на основе СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

Глава 3. Термины и определения

6. В настоящей Политике используются следующие основные термины, их сокращения и определения:
   1) Актив – все, что имеет ценность для Товарищества с точки зрения целей его деятельности и находится в его распоряжении;
   2) Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Товарищества, находящаяся в распоряжении Товарищества и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме;
   3) Бизнес-процесс – совокупность взаимосвязанных мероприятий или задач, направленных на создание определенного продукта или услуги для внешнего (клиент) или внутреннего (работник, СП Товарищества, другой бизнес-процесс) потребителя;
   4) ВНД – внутренний нормативный документ – внутренний документ установленной формы, утвержденный уполномоченным органом/лицом, регламентирующий нормы (правила) деятельности Товарищества, обязательный для соблюдения/применения, участниками отношений в рамках нормативно-регламентированной ситуации (Политика, Методика и т.д.);
   5) Высшее руководство – лицо или группа людей, осуществляющих руководство и управление Товариществом на высшем уровне;
   6) Доступность – свойство нахождения в состоянии готовности и пригодности для использования по запросу;

7) ИБ – Информационная безопасность – сохранение конфиденциальности, целостности и доступности информации;

8) ИС – Информационная система – приложения, службы, активы, связанные с информационными технологиями, или другие компоненты обработки информации;

9) Конфиденциальность – свойство, указывающее на то, что информация остается недоступной или нераскрытой для неавторизованных лиц, логических объектов или процессов;

10) Политика – намерения и направление Товарищества, официально сформулированные его высшим руководством;

11) Риск ИБ – риски воздействия преднамеренных и непреднамеренных угроз (ошибок в работе информационных систем, аварий, действий злоумышленников и т.д.), которые могут привести к нарушению конфиденциальности, доступности и/или целостности обрабатываемой информации.

Примечание: Риск ИБ определяется возможностью того, что угрозы будут использовать уязвимости информационных активов или группы информационных активов, что приведет к ущербу для Товарищества;

12) РК – Республика Казахстан;

13) СП – структурное подразделение, официально выделенная отдельная единица в организационной структуре по определенному участку деятельности Товарищества (департамент, отдел) с самостоятельными задачами, функциями и ответственностью за их выполнение с целью обеспечения реализации отдельных направлений деятельности Товарищества, осуществления функциональной ответственности за конкретное направление деятельности Товарищества, либо выполнения организационно-технического обеспечения реализации одного или нескольких направлений деятельности Товарищества;

14) Угроза – возможная причина нежелательного инцидента, который может нанести ущерб Товариществу;

15) Целостность – свойство сохранения полноты и точности.

Раздел 2. Основные положения

Глава 4. Цели и задачи ИБ

7. Для достижения и поддержания необходимого уровня ИБ в Товариществе разработана, внедрена, поддерживается и непрерывно совершенствуется ИБ в соответствии с требованиями Стандарта Республики Казахстан СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

8. Главной целью ИБ Товарищества является снижение вероятности нанесения материального, физического, репутационного или иного ущерба Товариществу, его партнёрам и клиентам в результате реализации угроз ИБ.

9. Указанная цель достигается посредством решения следующих задач:

1) своевременное выявление, оценка и прогнозирование источников угроз ИБ;

2) создание механизма оперативного реагирования на угрозы ИБ;
3) защита от вмешательства в процесс функционирования ИС посторонних лиц;
4) соответствие требованиям законодательства, регуляторов и договорным обязательствам в части ИБ;
5) обеспечение непрерывности критических бизнес-процессов;
6) достижение адекватности мер по защите от угроз ИБ;
7) изучение партнеров, клиентов, конкурентов и кандидатов на работу;
8) выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников;
9) повышение деловой репутации и корпоративной культуры.

Глава 5. Требования информационной безопасности

10. Построение ИБ Товарищества и ее функционирование осуществляется в соответствии со следующими основными требованиями:

1) вовлеченность высшего руководства. Деятельность по обеспечению ИБ инициирована и контролируется высшим руководством. Для обеспечения надлежащего уровня ИБ, содействия ее постоянному развитию и улучшению, высшее руководство обеспечивает:

- необходимыми ресурсами;
- разработку и совместимость политики и целей ИБ со стратегическим курсом Товарищества;
- интеграцию требований ИБ в процессы Товарищества;
- достижение ИБ своих ожидаемых результатов;
- донесение важности эффективного управления ИБ и выполнения всеми работниками, клиентами и контрагентами требований ИБ;
- распределение ролей и обязанностей между работниками Товарищества, связанными с ИБ, а также их надлежащее взаимодействие;
- регулярную оценку пригодности, релевантности и эффективности ИБ;

2) соответствие законодательным и нормативным актам РК, требованиям внешних регуляторов и договоров с контрагентами. Товарищество реализует меры обеспечения ИБ в строгом соответствии с действующим законодательством РК и договорными обязательствами;
3) соответствие ИБ высоким стандартам и лучшим практикам. Функционирование ИБ строится в соответствии с применимыми требованиями стандартов РК, международных стандартов, а также лучших мировых практик. В обязанности Товарищества входит постоянное улучшение эксплуатационных характеристик ИБ, расширение ее функций и повышение эффективности функционирования;
4) приоритетность. Классификация всех информационных активов Товарищества по степени важности и оценка реальных, а также потенциальных угроз ИБ;

5) реагирование на инциденты ИБ. Товарищество предпринимает действия по выявлению и оперативному реагированию на действительные, предпринимаемые и вероятные нарушения ИБ;

6) осведомленность в вопросах обеспечения ИБ. Требования в области ИБ доводятся до сведения всех работников, клиентов и контрагентов в части их касающейся. Текст Политики доступен всем заинтересованным сторонам;

7) компетентность персонала. Товарищество тщательно производит процедуру найма работников, повышает квалификацию, вырабатывает и поддерживает корпоративную этику, что создает благоприятную среду для деятельности и снижает риски ИБ. Товарищество на периодической основе осуществляет информирование и обучение работников по вопросам обеспечения ИБ;

8) персональная ответственность. Работники несут персональную ответственность за соблюдение требований ИБ. Обязанности по обеспечению ИБ также включаются в договоры с контрагентами;

9) взаимодействие и координация. Осуществление мер на основе четкой взаимосвязи СП Товарищества, сторонних организаций, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами;

10) экономическая обоснованность. Товарищество стремится выбирать меры обеспечения ИБ с учетом затрат на их реализацию, вероятности возникновения угроз ИБ и объема возможных потерь от их реализации. Проводится периодическая оценка эффективности используемых мер;

11) документированность. В Товариществе поддерживается документированность информации в объеме, необходимом для уверенности в выполнении процессов, как это было запланировано. Товарищество стремится, чтобы все требования в области ИБ были зафиксированы во внутренних документах, утвержденных высшим руководством;

12) разграничение пересекающихся обязанностей и предоставление минимально необходимых прав доступа. Противоречивые обязанности и области ответственности должны быть разделены с целью снижения возможностей для несанкционированных или непреднамеренных модификаций или некорректного использования активов Товарищества. Работникам и контрагентам предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств;

13) обязательность контроля. Контроль за деятельностью пользователей, а также мониторинг работы ИС должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия;

14) учет требований ИБ в проектной деятельности. Товарищество учитывает требования ИБ в проектной деятельности. Разработка и документирование требований по обеспечению ИБ осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

Глава 6. Средства управления информационной безопасностью

11. Основными мерами по обеспечению ИБ Товарищества являются:

1) **Административно-правовые и организационные меры** включают (но не ограничены ими):

- контроль исполнения требований законодательства РК и внутренних документов Товарищества;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников Товарищества работе с ИС и требованиям ИБ;
- реагирование на инциденты, локализацию и минимизацию последствий;
- анализ рисков ИБ;
- отслеживание и улучшение морального и делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников Товарищества.

2) **Меры физической безопасности** включают (но не ограничены ими):

- организацию пропускного и внутриобъектового режимов;
- построение периметра безопасности защищаемых объектов;
- организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
- организацию противопожарной безопасности охраняемых объектов;
- контроль доступа работников Товарищества в помещения ограниченного доступа.

3) **Программно-технические меры** включают (но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра;
- применение комплексно антивирусной защиты;
- использование средств ИБ, встроенных в ИС;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств;
- мониторинг состояния критичных элементов ИС.

Глава 7. Непрерывность бизнеса

12. В Товариществе внедрен процесс управления непрерывностью бизнеса с целью снижения убытков, вызываемых авариями и сбоями в ИС Товарищества до приемлемого уровня путем комбинирования предупреждающих и корректирующих мер.
13. В Товариществе разработаны и реализованы планы, которые позволят восстановить операции основных бизнес-процессов и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя. Планы аварийного восстановления должны регулярно тестироваться и пересматриваться.
14. Обеспечение непрерывности бизнеса описаны в соответствующих ВНД и направлены на снижение влияния чрезвычайной ситуации на жизнь и здоровье работников Товарищества, минимизацию влияния на клиентов, сохранение активов, оценку влияния чрезвычайной ситуации на деятельность Товарищества с целью ее скорейшего восстановления.

Раздел 3. Заключительные положения

Глава 8. Ответственность пользователей

15. Ответственность за обеспечение ИБ возлагается на все СП Товарищества в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.
16. Служба IT и ERP отвечает за координацию, контроль исполнения и актуальность настоящей Политики, а также за отчет о функционировании ИБ перед высшим руководством Товарищества.
17. Руководители всех СП отвечают:
    1) за своевременное доведение до сведения работников подотчетного(-ых) СП настоящей Политики;
    2) за выполнение работниками подотчетного(-ых) СП требований настоящей Политики Товарищества.
18. Все работники несут персональную ответственность за свои действия при работе в информационной инфраструктуре Товарищества и обращении с защищаемыми информационными активами Товарищества, а также за выполнение требований ИБ, установленных настоящей Политикой и ВНД, разработанными на ее основе.
19. Нарушение работником требований ВНД, разработанных на основе настоящей Политики, влечет за собой применение мер дисциплинарного воздействия в порядке, предусмотренном Трудовым кодексом РК.
20. Решение о применении и выборе мер ответственности принимается высшим руководством по результатам проведения служебного расследования в зависимости от целесообразности применения рассматриваемых мер, а также от сведений об умышленности нарушения.

Глава 9. Поддерживаемые записи

21. Записи, поддерживаемые на основании настоящий Политики:
    1. Лист регистрации изменений и дополнений в Политику информационной безопасности ТОО «Қамқор Менеджмент», указанный в Приложении 1 настоящей Политики;

2. Подтверждение ознакомления с Политикой информационной безопасности ТОО «Қамқор Менеджмент» по форме Приложения 2 настоящей Политики.

Глава 10. Срок действия и управление документом

22. Днем введения в действие Политики считать дату ее утверждения решением единственного участника Товарищества.

23. Владельцем настоящей Политики является Служба IT и ERP, который обязан проверять и по мере необходимости актуализировать документ как минимум 1 (один) раз в 2 (два) года.

24. Для оценки эффективности и релевантности настоящей Политики, необходимо рассматривать следующие критерии:

    1) случаи несоответствия и (или) изменения ИБ законодательным, нормативным, контрактным обязательствам и иным ВНД Товарищества;

    2) выявления снижения общего уровня ИБ Товарищества (по результатам внутреннего или внешнего аудита);

    3) существенные изменения организационной и (или) технологической инфраструктуры, ресурсов и бизнес-процессов Товарищества;

    4) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими ВНД Товарищества;

    5) учитывать предложения работников по улучшению или появление новых проверенных мировых практик и стандартов.

25. По вопросам, неурегулированным Политикой, руководствоваться следует иными документами Товарищества, регулирующими внутреннюю деятельность, положениями, правилами, инструкциями, распоряжениями и прочими актами, издаваемыми в Товариществе за подписью Генерального директора или иного уполномоченного в законодательном порядке лица, регулирующими вопросы обеспечения ИБ, и нормативно-правовыми актами РК.

26. Политика действует действуют до ее отмены, или признания утратившей силу отдельным решением единственного участника Товарищества, либо до утверждения решением единственного участника Товарищества новой редакции Политики. Изменения и дополнения в Политику вносятся путем издания ее в новой редакции и вступают в силу с даты их утверждения решением единственного участника Товарищества.

27. С момента утверждения настоящей Политики ранее действовавшая редакция Политики информационной безопасности Товарищества от 27 мая 2020 года считается утратившей силу.

Приложение № 1

к Политике информационной безопасности ТОО «Қамқор Менеджмент»

Лист регистрации изменений и дополнений в Политику информационной безопасности ТОО «Қамқор Менеджмент»

№	Номер редакции	№ раздела, подраздела, пункта, к которому относится вносимое изменение	Дата внесения изменения
1	2	3	4

Приложение № 2

к Политике информационной безопасности ТОО «Қамқор Менеджмент»
Подтверждение ознакомления с Политикой
информационной безопасности ТОО «Қамқор Менеджмент»

Подтверждение ознакомления с
Политикой информационной безопасности ТОО «Қамқор Менеджмент»

Я, _____,
(ФИО полностью)

_____
(наименование должности, структурного подразделения)

настоящим подтверждаю:

1. с Политикой информационной безопасности ТОО «Қамқор Менеджмент» ознакомлен _____
(подпись)
2. каждый пункт Политики информационной безопасности ТОО «Қамқор Менеджмент» мной понят _____
(подпись)

«_____» _____ 20_____ года
(дата)