УТВЕРЖДЕНА
решением Совета директоров
АО «КСЖ «Nomad Life»
Протокол № 231026/1
от «23» октября 2026 г.

ПОЛИТИКА

ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АО «КСЖ «Nomad Life»
И-205

г. Алматы, 2026 год

Данный документ поддерживается в электронном виде. После распечатки документ переходит в категорию неучитываемых экземпляров

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ 3
2. НОРМАТИВНЫЕ ССЫЛКИ 4
3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 4
4. ПРИНЦИПЫ ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 7
5. МЕХАНИЗМЫ РЕАЛИЗАЦИИ ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИИ И ПРАВИЛА КОНТРОЛЯ РИСКОВ 7
6. УПРАВЛЕНИЕ И ОТВЕТСТВЕННОСТЬ 11
7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 12
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ / ДОПОЛНЕНИЙ 13

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика ответственного использования искусственного интеллекта в АО «КСЖ «Nomad Life» (далее – Политика) определяет принципы и правила АО «КСЖ «Nomad Life» (далее – Общество) ответственного использования, проектирования, обучения, внедрения и эксплуатации систем искусственного интеллекта (далее – ИИ), а также комплексной минимизации специфических рисков ИИ, операционных рисков, киберрисков (рисков информационной безопасности) и поведенческих рисков Общества.

1.2. Политика является обязательной для исполнения всеми работниками Общества, членами органов управления, страховыми агентами, а также партнёрами, включая платформы и маркетплейсы (в части, относящейся к их взаимодействию с Обществом и предусмотренной договорами с ними). Требования Политики к обеспечению информационной безопасности и защите данных интегрируются в договоры и соглашения с внешними поставщиками ИТ-решений в части, применимой к предмету договора. При использовании стандартных (публичных) условий поставщиков облачных ИИ-сервисов допускается применение компенсирующих мер: обезличивание передаваемых данных, настройка запрета использования данных Общества для обучения моделей, ограничение состава передаваемых данных.

1.3. Целью Политики является построение эффективной и безопасной системы управления процессами разработки, внедрения и эксплуатации технологий ИИ, а также ограничение рисков ИИ в пределах утверждённого аппетита к риску Общества. Политика не ограничивает использование работниками Общества ИИ-ассистентов и иных ИИ-инструментов для повышения эффективности работы при соблюдении требований пунктов 5.4. и 5.5. Политики. Процессы управления рисками искусственного интеллекта на системной основе интегрируются в общую деятельность СУРиВК Общества.

1.4. Областью применения Политики является операционная деятельность Общества, в рамках которой осуществляются проектирование, сбор и подготовка данных, обучение, тестирование, внедрение, независимая валидация, мониторинг и вывод из эксплуатации систем ИИ (AI-систем).

1.5. Политика является внутренним нормативным документом Общества, имеющим статус открытого доступа, положения которого подлежат публичному раскрытию на официальном интернет-ресурсе Общества в качестве единого публичного документа о программе ответственного использования ИИ в Обществе.

1.6. **Программа ответственного использования ИИ.** Политика является программой ответственного использования ИИ Общества; отдельный документ с таким наименованием не разрабатывается. Программа включает следующие элементы:

1) ограничение доступа к чувствительным возможностям ИИ (подпункт 7) пункта 5.4. Политики);
2) маркировку контента, созданного ИИ, и информирование о решениях и взаимодействии с использованием ИИ (подпункты 4)–6) пункта 5.4. Политики);
3) механизмы выявления и коррекции дрейфа и деградации моделей ИИ (пункт 5.6. Политики);
4) периодическую оценку моделей ИИ на справедливость и отсутствие предвзятости (подпункт 1) пункта 5.3. Политики);
5) меры по снижению экологического следа вычислительной инфраструктуры и моделей ИИ, в том числе совместно с поставщиками (пункт 5.7. Политики);

6) процедуру обжалования решений, принятых с использованием ИИ, для клиентов и иных затронутых лиц (подпункт 4) пункта 5.1. Политики);
7) количественную оценку влияния ИИ на результаты в сфере устойчивого развития (пункты 5.8.–5.9. Политики);
8) обучение работников этичному и безопасному использованию ИИ (пункт 6.7. Политики);
9) развитие системы управления ИИ с учётом международных стандартов и возможность её внешней верификации (пункт 6.8. Политики).

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Политика разработана в соответствии с требованиями следующих нормативных правовых актов и внутренних документов Общества:

1) Закон Республики Казахстан «Об искусственном интеллекте»;
2) Закон Республики Казахстан «О страховой деятельности»;
3) Закон Республики Казахстан «О персональных данных и их защите»;
4) Закон Республики Казахстан «О защите прав потребителей»;
5) Закон Республики Казахстан «О масс-медиа»;
6) Постановление Правления Национального Банка Республики Казахстан от 27 августа 2018 года № 198 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для страховых (перестраховочных) организаций, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан»;
7) Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 3 августа 2026 года № 116 «Об утверждении Требований к управлению финансовыми продуктами, перечня финансовых продуктов (с указанием ставок и тарифов), об утверждении, изменении и прекращении предоставления которых субъект поведенческого надзора уведомляет уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций, правил такого уведомления, а также перечня документов и сведений, прилагаемых к уведомлению»;
8) Оценка рисков SRES/CRES. Методология модели и надзорные ожидания в отношении страхового рынка АРРФР (2026 год);
9) Иные нормативные правовые акты Республики Казахстан и внутренние нормативные документы Общества.

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1. В Политике используются следующие термины и определения:

1) **AI-система** – программное решение, модель, сервис или агент, использующий технологии ИИ и классифицируемый по уровням риска (минимальный, средний, высокий) в соответствии с законодательством Республики Казахстан;
2) **Владелец AI-системы** – ответственное лицо или структурное подразделение Общества, отвечающее за бизнес-результат, надлежащую эксплуатацию ИИ-алгоритма, мониторинг качества работы (для прогнозных моделей – метрик точности), а также управление модельным риском и рисками ИИ;

3) **Внутренний экономический капитал** – капитал, необходимый Обществу для покрытия существенных рисков, рассчитанный Обществом внутри системы управления рисками с использованием собственных актуарных моделей;
4) **Дистилляция знаний** – метод оптимизации и обучения систем ИИ, при котором компактная модель («ученик») обучается воспроизводить поведение и перенимать аналитические возможности более масштабной и вычислительно ёмкой модели («учителя») в целях снижения требований к аппаратным ресурсам;
5) **Заинтересованные стороны Общества** – физические и юридические лица, государственные органы (включая АРРФР), акционеры, работники и партнёры, чьи законные права и интересы учитываются Обществом при применении ИИ;
6) **ИИ-ассистент (вспомогательный ИИ-инструмент)** – внешний или внутренний сервис на основе генеративного ИИ (чат-боты, помощники для подготовки и анализа текста, кода, данных), используемый работником Общества для поддержки выполнения своих задач при условии, что результат проверяется работником и не используется для автоматического принятия решений в отношении клиентов. На ИИ-ассистенты не распространяются требования о назначении Владельца AI-системы, включении в Реестр моделей и независимой валидации; требования пунктов 5.4. и 5.5. Политики применяются к ним в полном объёме;
7) **Инференс (исполнение модели)** – этап жизненного цикла системы ИИ, в ходе которого промышленно развёрнутая и обученная модель применяется для обработки реальных входящих данных, генерации контента, прогнозирования или поддержки принятия операционных решений Общества;
8) **Искусственный интеллект (ИИ)** – технологии и системы, способные выполнять задачи, обычно требующие интеллектуальных функций человека, включая анализ данных, генерацию контента, прогнозирование, рекомендации и поддержку принятия решений;
9) **Квантование параметров модели ИИ** – метод оптимизации систем ИИ, заключающийся в снижении разрядности (точности) представления числовых значений весовых коэффициентов модели, направленный на уменьшение её объёма и повышение скорости выполнения вычислений;
10) **Мисселинг** – недобросовестная практика продаж, при которой клиенту через цифровые ИИ-каналы, сайты, партнёрские платформы или чат-боты предоставляется недостоверная, неполная или искажённая информация о страховом продукте, вводящая клиента в заблуждение относительно реальных условий, страховых премий, выкупных сумм и рисков;
11) **Независимая валидация** – объективная математическая, методологическая и технологическая проверка модели ИИ (включая проверку качества вводных данных, стабильности прогнозов и логики алгоритма), осуществляемая структурным подразделением или экспертами Общества, независимыми от процесса непосредственной разработки AI-системы. Для моделей ИИ внешних поставщиков (вендорских и облачных), внутренняя логика которых недоступна Обществу, независимая валидация ограничивается тестированием результатов работы модели на данных и сценариях Общества;
12) **Поведенческий риск** – риск возникновения негативных последствий для клиентов вследствие ненадлежащего дизайна и реализации страховых продуктов и услуг, недобросовестного ценообразования, непрозрачных условий, агрессивных или

дискриминационных практик продаж с использованием алгоритмов ИИ, а также создания барьеров при смене или прекращении обслуживания;

13) **Разработчик AI-системы** – работник Общества или внешний специалист, выполняющий технические задачи по разработке, настройке, интеграции, тестированию или сопровождению AI-системы в рамках поставленной задачи (технического задания, заявки или иного задания, оформленного в соответствии с внутренними документами Общества);
14) **Риск «чёрного ящика» (необъяснимости алгоритма)** – риск невозможности интерпретировать, логически обосновать или математически декомпозировать процесс принятия решения AI-системой (включая сложные нейросети) при тарификации, андеррайтинге или урегулировании убытков, что создаёт угрозу нарушения требований прозрачности перед клиентами и (или) АРРФР;
15) **Риск технологических галлюцинаций** – риск генерации моделями ИИ фактически недостоверной, искажённой или вымышленной информации, которая при предоставлении клиенту или интеграции во внутренние процессы приводит к мисселингу или операционным ошибкам;
16) **Риск цифровой дискриминации** – риск формирования AI-системой предвзятых или несправедливых результатов в отношении отдельных категорий клиентов (включая социально уязвимые слои населения, пенсионеров, лиц с инвалидностью) вследствие использования смещённых, неполных или некорректных исторических данных при обучении моделей;
17) **Риски ИИ** – комплекс технологических, комплаенс, правовых, операционных и этических рисков, возникающих на всех этапах жизненного цикла AI-систем, способных привести к финансовым убыткам Общества, нарушению прав клиентов, регуляторным санкциям со стороны АРРФР или репутационному ущербу;
18) **Структурное прореживание моделей (прунинг)** – метод оптимизации архитектуры нейронных сетей, заключающийся в направленном удалении избыточных, неиспользуемых или наименее значимых параметров (связей и нейронов) для снижения вычислительной сложности алгоритма без существенной потери точности его работы;
19) **Углеродный след вычислительной инфраструктуры** – совокупность выбросов парниковых газов, выраженная в эквиваленте диоксида углерода (CO_2-экв.), прямо или косвенно связанных с генерацией электроэнергии, потребляемой оборудованием в процессе обучения, тестирования и промышленной эксплуатации AI-систем Общества;
20) **Устойчивое развитие** – процесс изменений, при котором эксплуатация ресурсов, направление инвестиций, ориентация научно-технического развития и институциональные изменения согласованы друг с другом и укрепляют нынешний и будущий потенциал Общества для удовлетворения человеческих потребностей и устремлений.

3.2. В Политике используются следующие сокращения:

1) **АРРФР** – Агентство Республики Казахстан по регулированию и развитию финансового рынка;
2) **ВИЭ** – возобновляемые источники энергии;
3) **ИИ (AI)** – искусственный интеллект (Artificial Intelligence);
4) **ИТ** – информационные технологии;

5) **КИП** – корпоративный информационный портал;
6) **ПОДФТ/ФРОМУ** – противодействие легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения;
7) **СУРиВК** – система управления рисками и внутреннего контроля Общества;
8) **ЦОД** – центр обработки данных;
9) **ESG** – экологическое, социальное и корпоративное управление (устойчивое развитие);
10) **KPI** – ключевые показатели эффективности;
11) **PUE** – коэффициент эффективности использования энергии инфраструктурой центра обработки данных, определяемый как отношение общего объёма электрической энергии, потребляемой ЦОД, к энергии, расходуемой непосредственно ИТ-оборудованием.

4. ПРИНЦИПЫ ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

4.1. Для соблюдения законных прав и интересов заинтересованных сторон Общества при цифровом взаимодействии Общество применяет ИИ на основе четырёх главных принципов:

1) **Принцип этичности:** Общество стремится использовать ИИ исключительно во благо человека, стремясь к полному исключению цифровой дискриминации и ущемления прав граждан Республики Казахстан. Данный принцип ориентирован на всестороннюю защиту интересов клиентов Общества, включая социально уязвимые категории населения;
2) **Принцип прозрачности:** Общество стремится к обеспечению объяснимости и понятности работы алгоритмов для клиентов и регулятора в рамках доступных технологических возможностей, а также к поддержанию необходимой информационной открытости процессов для Единственного акционера Общества в целях эффективного корпоративного управления;
3) **Принцип безопасности:** Общество направляет усилия на обеспечение надёжной защиты обрабатываемых данных, повышение устойчивости систем к внешнему воздействию и сохранение контроля человека над критическими процессами;
4) **Принцип экологической устойчивости:** Общество признаёт влияние цифровых технологий на окружающую среду и стремится учитывать экологический след, связанный с обучением моделей ИИ и функционированием вычислительной инфраструктуры, отдавая приоритет энергоэффективным решениям и принципам «зелёного ИИ».

5. МЕХАНИЗМЫ РЕАЛИЗАЦИИ ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИИ И ПРАВИЛА КОНТРОЛЯ РИСКОВ

5.1. В рамках реализации принципов этичности, прозрачности и безопасности при использовании систем ИИ Общество обеспечивает защиту законных интересов и прав потребителей посредством внедрения следующих правил:

1) **Исключение полностью автоматических решений:** системы ИИ Общества не имеют права самостоятельно принимать окончательные решения, ограничивающие или прекращающие права клиентов;
2) **Контур обязательного человеческого контроля:** решение AI-системы, влекущее юридические последствия для клиента (отказ в заключении договора, отказ в страховой выплате или уменьшение её размера, расторжение договора), вступает в силу только после его проверки и подтверждения уполномоченным работником;
3) **Прозрачность и объяснимость алгоритмов:** Общество предоставляет клиентам по их запросу простые и понятные разъяснения о логике работы ИИ и возможных юридических последствиях обработки данных;
4) **Право на обжалование:** клиенты Общества и иные лица, в отношении которых принято решение с использованием ИИ (выгодоприобретатели, заявители, партнёры), имеют возможность через любой канал обслуживания Общества выразить несогласие с решением, принятым ИИ, и официально потребовать его перепроверки человеком. Такое обращение рассматривается с участием уполномоченного работника в сроки, установленные законодательством Республики Казахстан для рассмотрения обращений, а результат сообщается заявителю;
5) **Соблюдение установленных сроков:** Общество соблюдает сроки, установленные законодательством Республики Казахстан и внутренними документами Общества, при взаимодействии с потребителями и государственными органами.

5.2. Общество не допускает манипулятивные подходы и стремится к созданию честной цифровой среды посредством внедрения следующих правил:

1) **Запрет скрытых условий:** не допускается автоматическое включение платных опций и сопутствующих сервисов в договоры путём проставления электронных галочек по умолчанию;
2) **Отказ от необъяснимых алгоритмов:** Общество не использует для тарификации (ценообразования) и андеррайтинга модели, логику которых невозможно расшифровать и предоставить по требованию регулятора;
3) **Тестирование каналов взаимодействия:** Общество периодически, с периодичностью, определяемой Владельцем AI-системы с учётом уровня риска, проводит тестирование клиентских роботов и чат-ботов по набору контрольных сценариев силами подразделения, независимого от Владельца AI-системы, при необходимости включая выборочные контрольные закупки, для снижения риска технологических галлюцинаций и мисселинга;
4) **Исключение запрещённых практик:** Общество не использует ИИ для скрытого социального рейтингования потребителей или несанкционированного биометрического наблюдения;
5) **Соблюдение правил ПОДФТ/ФРОМУ:** алгоритмы ИИ не должны использоваться для блокировки или обхода обязательных комплаенс-проверок клиентов по спискам террористов.

5.3. В отношении AI-систем Общество применяет следующие защитные меры в той мере, в какой соответствующие системы используются:

1) **Цифровая справедливость:** AI-системы среднего и высокого уровней риска, влияющие на решения в отношении клиентов, оцениваются на предмет предвзятости результатов в отношении отдельных категорий клиентов в рамках оценки рисков по

пункту 6.3. Политики; при обучении собственных моделей проверяются обучающие данные.

2) **Обеспечение кибербезопасности ИИ:** AI-системы, размещённые в инфраструктуре Общества, защищаются в рамках общих мер информационной безопасности Общества; при использовании внешних ИИ-сервисов применяются требования пункта 5.5. Политики.
3) **Защита от недостоверной информации:** при использовании языковых моделей в клиентских каналах (чат-боты, голосовые помощники) их ответы об условиях страховых продуктов основываются на утверждённых материалах Общества; результаты работы ИИ-ассистентов, используемых работниками, проверяются работником.
4) **Минимизация технологической зависимости:** при использовании внешних ИИ-сервисов в AI-системах среднего и высокого уровней риска риск их недоступности учитывается в рамках действующих мер обеспечения непрерывности деятельности.

5.4. Общество соблюдает стандарты защиты конфиденциальности и прозрачности контента:

1) применяет обезличивание (маскирование, псевдонимизацию) персональных данных при их передаче во внешние ИИ-сервисы; обработка персональных данных AI-системами, размещёнными в инфраструктуре Общества, осуществляется в соответствии с внутренними документами Общества по защите персональных данных;
2) предоставляет работникам Общества доступ к AI-системам, обрабатывающим персональные данные, тайну страхования или коммерческую тайну, на основе принципа минимально необходимой производственной потребности; доступ к ИИ-ассистентам из Перечня разрешённых ИИ-сервисов предоставляется в соответствии с ролевой моделью по заявке руководителя подразделения;
3) размещает в рекламе, созданной ИИ, информацию об условиях, рисках и исключениях продукта в объёме, предусмотренном законодательством о рекламе и о страховой деятельности, либо ссылку на полные условия продукта;
4) информирует потребителя об использовании ИИ при принятии решений по его договору (заключение, тарификация, урегулирование) в порядке и форме, предусмотренных законодательством Республики Казахстан;
5) маркирует материалы в средствах массовой информации и социальных сетях, полностью сгенерированные ИИ без содержательной редакторской правки работником Общества, отметкой: ***«Контент создан системой искусственного интеллекта»*;**
6) информирует клиента о том, что он взаимодействует с ИИ (чат-бот, голосовой помощник), в начале взаимодействия и обеспечивает возможность перехода к общению с работником Общества;
7) ограничивает доступ к чувствительным возможностям ИИ (биометрическая идентификация, распознавание лиц, видеоаналитика, анализ эмоций): такие возможности применяются только при наличии законного основания и согласия субъекта данных, по коллегиальному решению с участием подразделений по информационной безопасности и комплаенсу, с предоставлением доступа ограниченному кругу уполномоченных работников.

5.5. Общество применяет следующие правила для минимизации рисков трансграничной утечки информации:

1) информация ограниченного доступа (персональные данные, тайна страхования, коммерческая тайна) передаётся во внешние ИИ-сервисы с соблюдением законодательства Республики Казахстан и внутренних документов Общества по защите информации и персональных данных. Персональные данные граждан Республики Казахстан передаются в зарубежные ИИ-сервисы в обезличенном виде либо на иных законных основаниях трансграничной передачи. Для рабочих задач используются корпоративные учётные записи; использование личных учётных записей для обработки информации ограниченного доступа не допускается. При выборе внешних ИИ-сервисов предпочтение отдаётся сервисам, условия использования которых исключают применение данных Общества для обучения моделей;
2) интеграция внешних ИИ-сервисов в информационные системы и бизнес-процессы Общества (в качестве AI-систем) осуществляется в порядке, установленном внутренними документами Общества для внедрения информационных систем и ИТ-решений. Использование ИИ-ассистентов работниками для выполнения своих задач отдельного согласования не требует при соблюдении требований подпункта 1) настоящего пункта;
3) работники Общества используют внешние ИИ-сервисы с соблюдением требований подпункта 1) настоящего пункта; при наличии сомнений в допустимости передачи информации в ИИ-сервис работник обращается в подразделение по информационной безопасности.

5.6. При использовании прогнозных моделей ИИ для принятия решений контроль качества их работы осуществляется в рамках СУРиВК в порядке и с периодичностью, определяемыми с учётом уровня риска системы. Такой контроль может включать сопоставление прогнозов с фактически наступившими событиями (бэк-тестинг) и отслеживание признаков дрейфа или деградации модели, при выявлении которых модель может быть перекалибрована, переобучена или выведена из эксплуатации.

5.7. Общество стремится:

1) учитывать, при наличии такой информации, показатели энергоэффективности центров обработки данных (например, PUE – Power Usage Effectiveness) при размещении ресурсоёмких AI-систем;
2) при разработке собственных моделей ИИ рассматривать методы оптимизации (квантование, дистилляция, прореживание), снижающие потребность в вычислительных ресурсах;
3) рассматривать наличие у поставщика экологических стандартов и использование возобновляемых источников энергии как дополнительный критерий при выборе облачных ИИ-сервисов и ИТ-инфраструктуры;
4) отдавать предпочтение готовым (предобученным) моделям и облачным ИИ-сервисам с разделяемой инфраструктурой вместо обучения и размещения собственных моделей, если это не противоречит требованиям безопасности и законодательства.

5.8. Оценка влияния ИИ на результаты Общества в сфере устойчивого развития (ESG) проводится по следующим показателям в той мере, в какой у Общества имеются соответствующие AI-системы и данные для их расчёта:

5.8.1. **В сфере экологической устойчивости (E):**

1) среднее значение PUE используемых центров обработки данных, если оно раскрывается провайдером (справочно);
2) доля собственных моделей ИИ, при разработке которых рассматривались методы оптимизации (при наличии собственных моделей).

5.8.2. **В сфере социальной ответственности (S):**

1) доля обращений клиентов об оспаривании решений, принятых с использованием ИИ, рассмотренных с участием работника в установленные сроки (при наличии таких обращений);
2) количество выявленных случаев предоставления клиентскими чат-ботами недостоверной информации и доля устранённых из них (при использовании клиентских чат-ботов).

5.8.3. **В сфере корпоративного управления (G):**

1) доля работников, вовлечённых в эксплуатацию AI-систем среднего и высокого уровней риска, прошедших обучение правилам безопасного и этичного использования ИИ;
2) доля AI-систем среднего и высокого уровней риска, прошедших независимую валидацию до вывода в промышленную среду.

5.9. Информация о значениях указанных показателей может включаться в отчётность о функционировании СУРиВК в установленном для неё порядке. Обобщённая информация о реализации Политики может раскрываться в годовом отчёте Общества и (или) отчёте об устойчивом развитии.

6. УПРАВЛЕНИЕ И ОТВЕТСТВЕННОСТЬ

6.1. Зоны ответственности при использовании ИИ распределяются между участниками, указанными в пунктах 6.2.–6.6. Политики.

6.2. Правление и Совет директоров Общества осуществляют общее руководство вопросами ответственного использования ИИ в рамках своей компетенции, определённой законодательством Республики Казахстан и уставом Общества, в том числе при утверждении аппетита к риску Общества.

6.3. Оценка рисков AI-систем среднего и высокого уровней риска до их ввода в промышленную эксплуатацию и учёт таких систем осуществляются в рамках СУРиВК в порядке, установленном внутренними документами Общества по управлению рисками.

6.4. Владелец AI-системы среднего или высокого уровня риска отвечает за её использование по целевому назначению и за прохождение оценки рисков, предусмотренной пунктом 6.3. Политики.

6.5. Технические специалисты и разработчики несут персональную ответственность исключительно за качественное выполнение ИТ-задач в рамках поставленной задачи (технического задания, заявки или иного задания).

6.6. Работники Общества соблюдают требования Политики. Работник Общества не несёт ответственности за системные ошибки ИИ, сбои, некорректные результаты работы системы ИИ или внешних поставщиков, если его действия (бездействие) соответствовали установленным инструкциям и процедурам. При выявлении критической угрозы, связанной с использованием системы ИИ, работник имеет право временно приостановить соответствующую операцию до получения указаний от уполномоченного лица или подразделения.

6.7. Общество способствует повышению осведомлённости работников об ответственном использовании ИИ. Вопросы безопасного и этичного использования ИИ, защиты персональных данных при работе с ИИ-сервисами и выявления рисков недостоверной информации могут включаться в действующие программы обучения работников (в том числе по информационной безопасности и защите персональных данных), а также доводиться до работников в виде информационных и методических материалов на КИП.

6.8. При развитии практик управления ИИ Общество может ориентироваться на международные стандарты в этой области (в том числе ISO/IEC 42001) и по решению Правления проводить независимую внешнюю оценку таких практик.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Владельцем Политики является подразделение Общества, ответственное за управление рисками, при участии подразделения, ответственного за цифровую трансформацию и развитие технологий искусственного интеллекта, которое отвечает за своевременную актуализацию и мониторинг применимости настоящего документа.

7.2. Политика утверждается решением Совета директоров Общества, вступает в силу и становится обязательной для исполнения с даты, указанной в решении Совета директоров Общества, и действует до её отмены или замены новой.

7.3. Политика пересматривается по мере необходимости для обеспечения её актуальности и соответствия требованиям законодательства Республики Казахстан и внутренних документов Общества.

7.4. Внесение изменений и дополнений в Политику осуществляется в соответствии с внутренними документами Общества.

7.5. Все изменения в Политику доводятся до сведения работников путём публикации на КИП и рассылки уведомлений.

7.6. Оригинал Политики на бумажном носителе хранится в подразделении методологии.

7.7. Электронная версия Политики размещается на КИП подразделением методологии.

7.8. Положения, не урегулированные Политикой, регулируются в соответствии с законодательством Республики Казахстан и/или внутренними документами Общества.

7.9. В случае, если какие-либо нормы Политики противоречат законодательству Республики Казахстан, то применяются нормы законодательства Республики Казахстан.

7.10. Если в результате изменений в законодательстве Республики Казахстан отдельные положения Политики вступают с ним в противоречие, они утрачивают силу до внесения соответствующих изменений.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ / ДОПОЛНЕНИЙ

№	Дата введения изменения / дополнения	№ пункта документа, к которому относится изменение / дополнение	Лист (стр.) документа	Основание (№ и дата решения)