Утверждена
Президентом
АО «Товарная биржа «Каспий»
Приказ №19/1-П
от «03» февраля 2025 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вводится в действие с «03» февраля 2025 года
взамен Политики информационной безопасности АО «Товарная биржа «Каспий»,
утвержденной приказом Президента от «01» июня 2022 года №33/1-П

https://ccx.kz/

г. Астана | 2025 год

1. Назначение

1.1. Настоящая Политика информационной безопасности (далее - Политика) акционерного общества «Товарная Биржа «Каспий» (далее - Организация) определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ.

1.2. Настоящая Политика утверждается решением Правления Организации. Изменения и дополнения в настоящую Политику вносятся решением Правления Организации.

1.3. Если один из пунктов настоящей Политики становится недействительным, то это не затрагивает другие пункты Политики. Недействительный пункт исключается или заменяется другим пунктом, допустимым в правовом отношении.

1.4. Если в результате изменения законодательства Республики Казахстан отдельные пункты настоящей Политики вступают в противоречие с ним, эти пункты утрачивают силу и до момента внесения изменений и дополнений в Политику, необходимо руководствоваться требованиями законодательства Республики Казахстан.

2. Область распространения

2.1. Настоящая Политика распространяется и обязательна к применению всеми структурными подразделениями Организации, подлежит соблюдению и применению всеми работниками Организации.

2.2. Положения настоящей Политики применимы ко всем информационно-коммуникационным технологиям и телекоммуникационным ресурсам, используемым в Организации, а также помещениям, в которых пользователь может получить доступ к информационным системам и информационно-коммуникационной инфраструктуре Организации.

2.3. В целях обеспечения выполнения положений настоящей Политики необходимо обеспечить её соблюдение третьей стороной. Поэтому, в соответствующих случаях все договоры (соглашения) должны содержать требование о соблюдении требований настоящей Политики. Вся деятельность, подразумевающая контакт третьей стороны с данными, содержащимися в информационных системах и электронных информационных ресурсах, должна осуществляться в соответствии с требованиями настоящей Политики. Данное требование распространяется на всех работников третьей стороны. Своевременное уведомление третьих лиц о необходимости соблюдения требований настоящей Политики является обязанностью всех структурных подразделений Организации, занимающихся подготовкой договоров.

3. Термины, определения и сокращения

3.1. В настоящей Политике использованы следующие термины и соответствующие им определения:

3.1.1. **авторизованный пользователь** - пользователь информационных систем, использующихся в Организации, который ранее проходил процесс регистрации и на данный момент зашел под своей учетной записью;

3.1.2. **информационная безопасность в сфере информатизации -** состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;
3.1.3. **информационные активы -** данные с реквизитами, которые позволяют провести идентификацию, и имеют ценность для определенной организации и находятся в ее распоряжении;
3.1.4. **информационная система** - организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;
3.1.5. **специалист по ИБ** - специалист Организации, ответственный за управление мероприятиями в области информационной безопасности;
3.1.6. **обеспечение информационной безопасности** - сохранение ее конфиденциальности, целостности и доступности;
3.1.7. **администратор** - работник Организации или службы технической поддержки, представляющий услуги системного администрирования и технической поддержки IT-инфраструктуры Организации в рамках договорных отношений;
3.1.8. **база данных** - совокупность данных организованных согласно концептуальной структуре, описывающий характеристику этих данных, а также взаимосвязи между их объектами;
3.1.9. **системный журнал** - хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий;
3.1.10. **IT-инфраструктура** - инфраструктура, состоящая из интегрированного комплекса серверного оборудования, сетевого оборудования, информационных систем, программ, сетевых и системных служб;
3.1.11. **кроссовое помещение** - помещение, предназначенное для распределительных устройств сетей телекоммуникаций;
3.1.12. **доступность** - гарантия того, что авторизованные пользователи всегда получат доступ к данным;
3.1.13. **конфиденциальность** - свойство информации, гарантирующее, что доступ к информации имеет только определенные лица;
3.1.14. **инцидент** - любое непредвиденное или нежелательное событие, которое может нарушать деятельность или информационную безопасность;
3.1.15. **уязвимость** - слабое место в информационной системе, которое может привести к нарушению безопасности;
3.1.16. **пользователь** - субъект информатизации, использующий объекты информатизации для выполнения конкретной функции и (или) задачи, в том числе работники Организации;

3.1.17. **серверное помещение** - помещение, предназначенное для размещения серверного, активного и пассивного сетевого (телекоммуникационного) оборудования и оборудования структурированных кабельных систем;
3.1.18. **служба технической поддержки** - работники Организации и/или юридические лица, осуществляющие системно-техническое обслуживание программно-аппаратных средств, внедрение и (или) сопровождение информационных ресурсов;
3.1.19. **целостность** - гарантия сохранности данных, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.
3.1.20. **третья сторона** - лицо или орган, признаваемые независимыми от участвующих сторон в рассматриваемом вопросе;
3.1.21. **электронные информационные ресурсы** - информация, предоставленная в электронно-цифровой форме и содержащаяся на электронном носителе, интернет - ресурсе и (или) в информационной системе;
3.1.22. **служебная информация** - к служебной информации могут быть отнесены любые сведения, относящиеся к деятельности подразделений Организации, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для Организации.
3.2. В настоящей Политике использованы следующие сокращения:
3.2.1. **ИБ** – информационная безопасность;
3.2.2. **ИС** – информационные системы;
3.2.3. **ЭИР** – электронные информационные ресурсы;
3.2.4. **СВТ** – средства вычислительной техники;
3.2.5. **ПО** – программное обеспечение;
3.2.6. **ЛВС** – локально-вычислительная сеть;
3.2.7. **НСД** – несанкционированный доступ;
3.2.8. **ИБП** – источник бесперебойного питания.

4. Нормативные ссылки

4.1. В настоящей Политике использованы ссылки на следующие нормативные правовые акты Республики Казахстан и внутренние документы Организации:
4.1.1. Закон РК «Об информатизации»;
4.1.2. Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832;
4.1.3. СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;
4.1.4. СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;
4.1.5. СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;

4.1.6. национальный стандарт СТ РК ISO/IEC 27001-2023 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования»;
4.1.7. СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью»;

5. Описание деятельности

5.1. Цель и задачи обеспечения информационной безопасности

5.1.1. Целью обеспечения информационной безопасности является предотвращение и минимизация ущербов от реализации внешних или внутренних угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации Организации.
5.1.2. Задачами обеспечения информационной безопасности являются:
5.1.2.1. защита конфиденциальности данных – доступ только у лиц, имеющих на это полномочия;
5.1.2.2. доступность информационных систем с находящимися в них данными конкретным пользователям, у которых есть право доступа к таким сведениям;
5.1.2.3. целостность данных – предполагает блокировку несанкционированного изменения информации;
5.1.2.4. обеспечение непрерывности деятельности Организации, организационно-методическими и техническими мероприятиями, направленными на минимизацию последствий утраты информационных активов посредством комбинации предупреждающих и восстанавливающих мер и мероприятий;
5.1.2.5. управление рисками в целях недопущения или снижения вероятности возникновения внештатных ситуаций;
5.1.2.6. выявление и недопущение нарушений информационной безопасности, а также условий для их реализации;
5.1.2.7. создание механизма оперативного мониторинга на инциденты информационной безопасности и реагирования на нарушения.

5.2. Основные принципы обеспечения информационной безопасности

5.2.1. Основным принципом обеспечения ИБ является защита ИС и ЭИР от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования или несанкционированного доступа к циркулирующей в ней информации или незаконного ее использования.
5.2.2. Защита ИС и ЭИР достигается посредством обеспечения и постоянного поддержания следующих свойств:
5.2.2.1. доступность обрабатываемой информации;
5.2.2.2. обеспечение конфиденциальности информации, хранимой, обрабатываемой СВТ и передаваемой по каналам связи;

5.2.2.3. целостность и аутентичность (подтверждение авторства) информации, хранимой и обрабатываемой и передаваемой по каналам связи.
5.2.3. Для обеспечения указанных свойств Организация должна обеспечивать эффективное решение следующих задач:
5.2.3.1. защита от вмешательства в процесс функционирования посторонних лиц (авторизация, т.е. возможность использования информационных систем, наличие доступа к ее ресурсам только у зарегистрированных в установленном порядке пользователей);
5.2.3.2. разграничение доступа зарегистрированных пользователей к информационным ресурсам;
5.2.3.3. регистрация действий пользователей информационных систем при использовании защищаемых ресурсов в системных журналах и периодический контроль корректности действий пользователей информационных систем путем анализа содержимого этих журналов ответственным лицом по ИБ;
5.2.3.4. контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
5.2.3.5. защита от несанкционированной модификации и контроль целостности ИС и ЭИР, а также системы от внедрения несанкционированных программ, включая компьютерные вирусы;
5.2.3.6. защита конфиденциальной информации, информации с ограниченным доступом, персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи, а также от несанкционированного разглашения или искажения;
5.2.3.7. обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
5.2.3.8. своевременное выявление внешних или внутренних источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба Организации, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
5.2.3.9. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

5.3. Распределение обязанностей по обеспечению информационной безопасности

5.3.1. Ответственный специалист по ИБ обязан обеспечить реализацию комплекса мероприятий по поддержанию необходимого уровня ИБ Организации посредством предоставления четких указаний, принятия обязательств, постановок задач и осведомленности пользователей об обязанностях по обеспечению ИБ.
5.3.2. Компетенция Президента Организации:
5.3.2.1. курирование деятельности ответственного лица по ИБ;
5.3.2.2. обеспечение эффективной работы ответственного лица по ИБ в соответствии с поставленными задачами и функциями;
5.3.2.3. контроль за деятельностью ответственного лица по ИБ ;

5.3.2.4. четкое управление и реальная поддержка инициатив в области ИБ;
5.3.2.5. иные функции, предусмотренные внутренними документами Организации.
5.3.3. Компетенция членов Правления Организации:
5.3.3.1. обеспечение оказания содействия в вопросах соблюдения требований ИБ курируемыми структурными подразделениями аппарата Правления Организации;
5.3.3.2. пересмотр эффективности реализации настоящей Политики в рамках компетенции;
5.3.3.3. иные функции в рамках компетенции, предусмотренные внутренними документами Организации.
5.3.4. Ответственный специалист по ИБ несет ответственность за несоблюдение Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности и настоящей Политики.
5.3.5. Администраторы ИС обязаны действовать согласно внутренним документам Организации. Администратор ИС при нарушении требований ИБ Организации, в соответствии с зонами их ответственности, будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством РК, а также внутренними нормативными документами Организации.
5.3.6. Руководители структурных подразделений Организации обеспечивают контроль выполнения всех пунктов данной Политики. Руководители несут персональную ответственность за выполнение требований информационной безопасности и соблюдение Политики в возглавляемых ими подразделениях.
5.3.7. Работники - пользователи ИС, использующихся в Организации, обязаны действовать согласно своим должностным обязанностям и внутренним документам Организации в сфере ИБ, в т.ч.:
5.3.7.1. выявление и предотвращение реализации угроз ИБ в рамках своей компетенции;
5.3.7.2. реагирование на инциденты ИБ;
5.3.7.3. прогнозирование и предупреждение инцидентов ИБ в пределах своей компетенции;
5.3.7.4. мониторинг и оценка ИБ в рамках своего участка работы (рабочего места, СП) в пределах своей компетенции;
5.3.7.5. выполнение требований обеспечения ИБ, включая обязательства по неразглашению конфиденциальной информации.

5.4. Координация информационной безопасности

5.4.1. Действия работников Организации в части обеспечения ИБ должны координироваться Президентом Организации либо его заместителем в рамках своей компетенции в соответствии с их компетенцией.
5.4.2. Координация ИБ должна включать взаимосвязь и сотрудничество пользователей, администраторов, разработчиков прикладного программного обеспечения и кадровых подразделений.
5.4.3. При координации ИБ:

5.4.3.1. должно обеспечиваться соответствие выполняемых мероприятий по обеспечению ИБ настоящей Политике;
5.4.3.2. должны определяться мероприятия по обеспечению ИБ в случае несоответствия угроз настоящей Политике;
5.4.3.3. должны идентифицироваться все изменения угроз ИБ и степень уязвимости информации и средств обработки информации к угрозам ИБ;
5.4.3.4. должна оцениваться адекватность принимаемых решений и координировать реализацию мер контроля ИБ;
5.4.3.5. должен повышаться профессиональный уровень пользователей за счет обучения, подготовки по ИБ и осведомленности о ней;
5.4.3.6. должна оцениваться информация, полученная в ходе мониторинга и просмотра инцидентов по ИБ и рекомендовать соответствующие мероприятия в ответ на идентифицированные инциденты ИБ.

5.5. Обучение и осведомленность в вопросах информационной безопасности

5.5.1. Требования к обучению и осведомленности в вопросах ИБ:
5.5.1.1. работники Организации, службы технической поддержки и администраторы должны быть ознакомлены с настоящей Политикой;
5.5.1.2. ответственный по ИБ должен проводить первичный инструктаж по ИБ для вновь принятых работников Организации и фиксировать в Журнале инструктажа по ИБ;
5.5.1.3. работники службы технической поддержки и администраторы, обеспечивающие функционирование IT-инфраструктуры Организации, должны проходить инструктаж по соблюдению требований ИБ не реже одного раза в год;
5.5.1.4. в целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьими лицами мероприятия по управлению ИБ Организации;
5.5.1.5. ответственные работники по ИБ проходят специализированные курсы в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата;
5.5.1.6. работники службы технической поддержки и администраторы обязаны незамедлительно сообщать о любых нарушениях в сфере ИБ ответственным по ИБ;
5.5.1.7. ответственные работники по ИБ должны вести мониторинг посещений серверного (кроссового) помещений Организации, посредством журнала посещения серверного (кроссового) помещения;

5.6. Управление инцидентами

5.6.1. В случае обнаружения нарушения ИБ все пользователи ИС и ЭИР, используемыми в деятельности Организации, обязаны незамедлительно доложить ответственным работникам по ИБ, непосредственному руководителю и по возможности обеспечить минимизацию ущерба.

5.7. Меры по реализации Политики информационной безопасности

5.7.1. Меры по защите информации от утечки по техническим каналам их передачи.

Для выявления утечки информации, необходим систематический контроль возможности образования каналов утечки и оценки их опасности на границах контролируемой зоны (территории, помещения). Закрытие и локализация технических каналов утечки информации обеспечивается организационно-техническими мерами.

В соответствии с используемыми каналами передачи информации предусматриваются технические средства защиты. Организуется система регистрации, передачи, приема и хранение носителей информации, предусматриваются способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими средствами защиты.

Защита информации от утечки по каналам их передачи достигается путем применения комплексных программных, технических средств защиты и организационных мер.

5.7.2. Меры по защите СВТ:

5.7.2.1. защита от НСД к СВТ. Строится по нескольким направлениям: осуществляется регистрация пользователей, блокирование учетных записей, парольная защита. Определяются организационные меры по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя СВТ;

5.7.2.2. защита от использования незарегистрированных носителей информации. Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации. За запись служебной и иной защищаемой информации на незарегистрированные в установленном порядке носители, пользователь привлекается к дисциплинарной ответственности.

5.8. Меры по защите информации

5.8.1. Для защиты от нелегального внедрения и использования неучтенного ПО, кроме физической защиты СВТ, входит проведение аудита и мониторинг системных журналов, устанавливается базовый комплекс ПО, который необходимо устанавливать на рабочие станции пользователей.

5.8.2. Новые средства должны соответствующим образом быть одобрены со стороны председателя Правления либо его заместителя в рамках своей компетенции и администраторов средств управления, авторизующих их цель и использование, при этом аппаратные средства и ПО проверяются на совместимость с другими компонентами системы. Согласование следует также получить от руководителя ответственного лица по ИБ, чтобы обеспечить уверенность в том, что все соответствующие политики безопасности и требования соблюдены.

5.8.3. Копирование и передача служебной и иной защищаемой информации третьим лицам подлежит только с разрешения председателя Правления Организации.

5.8.4. За копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения Президента, пользователь привлекается к дисциплинарной ответственности.
5.8.5. Защита информации достигается путем ограничения физического доступа к средствам отображения информации, исключения наблюдения, за отображаемой информацией, посторонними лицами.
5.8.6. Персональные компьютеры и принтеры не должны оставаться без присмотра во время обработки информации и должны защищаться паролями или иными методами на время отсутствия пользователя. Доступ к каждому рабочему месту, на котором обрабатывается служебная информация, должен быть физически ограничен и предоставлен только тем пользователям, которым необходимо знать данную информацию. Если служебная информация не используется, она всегда должна быть защищена от неправомочного раскрытия. Служебная информация ограниченного доступа в бумажной форме должна храниться в сейфах. Сотрудники должны размещать экраны компьютеров таким образом, чтобы предотвратить несанкционированный просмотр служебной информации.
5.8.7. В целях защиты информации от действий вредоносных программ и вирусов используются программные средства, специальные программы-анализаторы, осуществляющие постоянный контроль за возникновением отклонений в деятельности прикладных программных продуктов, периодическую проверку наличия возможных следов вирусной активности, а также входной контроль новых программ и внешних носителей перед их использованием.
5.8.8. Организационные меры, включают в себя разработку нормативно - правовых актов, регламентирующие эту деятельность, и проведение работ в соответствии с ними.
5.8.9. Сотрудники внешних организаций (разработчики, программисты, технический персонал и т.д.), пропускаются в здания в соответствии с инструкциями о пропускном и внутриобъектовом режиме на данных объектах только в сопровождении ответственных работников Организации. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику внешних организаций, допускаемого к работе с конкретной ИС, должна подаваться заявка на регистрацию пользователя с предоставлением доступа к информационным ресурсам согласно «Правил организации процедуры аутентификации».
5.8.10. В целях осуществления и поддержания соответствующего уровня информационной безопасности при использовании услуг, предоставляемых третьей стороной, необходимо проверять наличие в договорных обязательствах соглашений требований по вопросам ИБ, осуществлять мониторинг соответствия соглашений и управлять изменениями, гарантирующими, что предоставляемые услуги удовлетворяют всем требованиям соглашения с третьей стороной.
5.8.11. До начала этапа эксплуатации автоматизированной системы ее пользователи, а также необходимый руководящий и обслуживающий персонал

должны пройти инструктаж. Ознакомиться с перечнем сведений, относящихся к коммерческой тайне и конфиденциальным сведениям в Организации, в части их касающейся, а так же своим уровнем полномочий, организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного распространения.

5.8.12. Для защиты от хищения носителей информации, устанавливается определенный порядок хранения и использования носителей информации, в том числе сведений в электронном виде. При передаче носителя цифровой информации, для повторного использования за пределами организации, проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений.

5.8.13. Для защиты информации, хранящейся на СВТ, за каждым СВТ закрепляется работник Организации, который принимает СВТ под роспись согласно паспорта СВТ. На СВТ используется система аутентификации работника, работающего на нем. Передача СВТ в пользование другому работнику осуществляется с разрешения руководителя структурного подразделения.

5.8.14. Защита от умышленной модификации информации, кроме средств регламентированного доступа к СВТ, осуществляется программными, техническими и организационными мерами. Для своевременного выявления и обнаружения указанных посягательств используются журналы действий пользователей и администраторов.

5.8.15. Действия работников по сопровождению серверов должны быть регламентированы. При нарушении регламента, причастные работники должны привлекаться к дисциплинарной ответственности.

5.8.16. Для защиты от сбоев и НСД к коммуникационным средствам, основные и резервные телекоммуникационные сервисы физически отделяются друг от друга.

5.8.17. Защита коммуникаций от незаконного подключения, кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся необходимые мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц, по получению доступа к коммуникациям. За незаконное подключение и попытку незаконного подключения к линиям связи и сетевому оборудованию, лица несут ответственность в соответствии с действующим законодательством.

5.8.18. Для защиты от неправомерного включения, выключения оборудования корпоративной вычислительной сети, эксплуатация оборудования сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, который работает в соответствии с указанием руководства.

5.8.19. Защита от неправомерной модификации передаваемых данных, технической и служебной информации, кроме средств санкционированного

доступа к коммуникационным средствам и сетевому оборудованию, осуществляется программно-техническими и организационными мерами.
5.8.20. Для защиты системы архивирования определяется порядок резервного копирования, хранения и восстановление программных продуктов и информационных систем (порядок описан в «Регламент резервного копирования и восстановления информации Организации».
5.8.21. Для обеспечения защиты информации в корпоративной вычислительной сети, удаленный доступ из внешней среды по различным каналам связи к серверному и коммуникационному оборудованию запрещен.
5.8.22. Все вспомогательные коммунальные услуги, такие как электричество, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха должны быть адекватны системам, которые они обслуживают. Вспомогательные коммунальные услуги должны проходить регулярную проверку и, по возможности, испытание с целью обеспечения их должного функционирования и понижения риска их неправильного срабатывания или сбоев. Необходимо наличие источника питания, технические данные которого соответствуют спецификациям производителя оборудования. Необходимо обеспечивать надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования. Оборудование, поддерживающее критические бизнес процессы, необходимо подключать через ИБП. Оборудование ИБП следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.
5.8.23. Детальное описание процедур обеспечения ИБ в Организации изложено в технической документации по информационной безопасности, разработанной в реализацию требований пунктов 33-34 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, а также ВНД Организации, отражающей отдельные аспекты защиты информации.

5.9. Оценка рисков и пересмотр Политики информационной безопасности

5.9.1. Соблюдение требований Политики информационной безопасности обязательно для всех работников Организации. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации.
5.9.2. Результаты аудита служат основанием оценки рисков, их идентификации, определения количества и порядка очередности, согласно критериям допустимости риска и задач, актуальных для Организации. Результаты должны направлять и определять надлежащие действия Руководства, а также приоритеты для управления рисками информационной безопасности, необходимых к внедрению элементов управления, отобранных для зашиты этих рисков.
5.9.3. Оценка рисков должна проводиться на регулярной основе не менее 1 раза в год, для своевременного реагирования на изменения рисков и требований по безопасности.

5.9.4. Результаты аудита, а также обратная связь со стороны пользователей могут служить основанием для пересмотра некоторых положений Политики и внесения в них необходимых корректировок.
5.9.5. Ответственный специалист по ИБ не менее 1 раза в два года, должен проводить пересмотр Политики, на предмет соответствия предъявляемым требованиям, и в случае возникновения необходимости, при выявлении в процессе аудита несоответствия современным требованиям, вносить изменения и дополнения.
5.9.6. Кроме этого, используемые информационные технологии и организация служебной деятельности непрерывно меняются, это приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности.
5.9.7. Любые изменения в данной Политике должны быть санкционированы Президентом Организации.

5.10. Ответственность и контроль

5.10.1. Ответственность за обеспечение реализации, информационного сопровождения, развития и актуализации настоящей Политики, а также мониторинг исполнения ее положений возлагается на ответственного специалиста по ИБ.
5.10.2. Ответственность за планирование и мониторинг состояния ИБ и ее эффективности в Организации возлагается на ответственного специалиста по информационной безопасности.
5.10.3. Пользователи ИС и ЭИР несут ответственность за неисполнение и/или ненадлежащее исполнение требований настоящей Политики, за все действия, связанные с использованием СВТ, ЛВС. За действия, связанные с настройкой сетевых параметров, несет ответственность администратор сети. Политика обязательна для исполнения всеми лицами, работающими с инфраструктурой Организации.
5.10.4. В случае нарушения требований настоящей Политики, пользователи ИС и ЭИР привлекаются к дисциплинарной, административной или иной ответственности в соответствии с требованиями законодательства Республики Казахстан, а также внутренними нормативными документами Организации.
5.10.5. Сотрудники сторонних организаций допустившие нарушения требований настоящей Политики несут ответственность в соответствии с договорными отношениями.
5.10.6. Контроль за выполнением требований настоящей Политики осуществляет ответственный специалист по ИБ.

ЛИСТ ОЗНАКОМЛЕНИЯ

№	ФИО	Должность	Личная подпись	Дата
1	Кадисов М.М.	Президент		03.02.2025
2	Айнабеков Ж.С.	Начальник отдела комплаенса и управление рисками		03.02.2025
3	Ахметов А.Х.	Начальник юридического отдела		03.02.25
4	Жақыпбек Г.М.	Бухгалтер		03.02.2025
5	Жантас Н.О.	Начальник отдела аналитики и мониторинга торгов		03.02.2025
6	Искаков А.Р.	Советник президента		
7	Ізімова П.А.	Маклер		03.02.25
8	Казыбаев Қ.М.	Бизнес-аналитик		03.02.25
9	Нургалиева Ж.К.	Главный бухгалтер		03.02.25
10	Сиренко В.В.	Специалист по информационной безопасности		03.02.25
11	Сулейменова Ж.Д.	Начальник отдела маклериата		03.02.25
12	Тюлемисова Д.Б.	Руководитель отдела информационных технологий		03.02.25
13	Хворов П.А.	Вице-президент		03.02.25
14	Шукаева А.М.	Водитель		03.02.25