«УТВЕРЖДЕНО»
приказом №
от « » _____2025 года
Ген. директора ОсОО «Амана обмен виртуальных активов»

Общество с ограниченной ответственностью «Амана обмен виртуальных активов»

Правила, направленные на обеспечение выполнения требований законодательства о противодействии легализации доходов, полученных от преступной деятельности, и финансированию терроризма

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящие Правила разработаны в соответствии с Законом Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов» (далее - Закон «О ПФТД/ЛПД») и другими нормативно-правовыми актами Кыргызской Республики.

1.2. Целью настоящих Правил является определение минимальных требований по организации внутреннего контроля в Организации в целях ПФТД/ЛПД, а также проведению операций, имеющих признаки подозрительных операций.

1.3. Компания ОсОО «Амана обмен виртуальных активов» (далее - Компания) строго соблюдает законодательство Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов (ПФТД/ЛПД).

2. ДЕЯТЕЛЬНОСТЬ КОМПАНИИ В ОБЛАСТИ ПФТД/ЛПД

2.1. При регистрации и обслуживании клиентов в Компании строго соблюдаются требования KYC, что предполагает сбор и проверку исчерпывающих данных, необходимых для идентификации личности. Клиент обязан предоставить полное имя, дату рождения, гражданство, а также документ, удостоверяющий личность (паспорт или иной документ с указанием номера, серии, даты выдачи и подтвержденный фотографией), дополненный актуальным адресом проживания и контактной информацией. Помимо этого, запрашиваются сведения о роде деятельности клиента и источниках происхождения его средств. Эти меры соответствуют как международным стандартам, в том числе рекомендациям FATF, так и требованиям национального законодательства, регулируемого Законом Кыргызской Республики от 6 августа 2018 года №87 «О противодействии легализации (отмыванию) преступных доходов и финансированию терроризма».

2.2. Компания применяет настоящие Правила для выполнения следующих основных обязанностей:

1) осуществление мер по выявлению, оценке, мониторингу, управлению, снижению и документированию рисков; снижению и документированию рисков;
2) осуществление мер надлежащей проверки клиентов;
3) применение целевых финансовых санкций и приостановление операций (сделок);
4) применение мер в отношении высокорискованных стран;
5) своевременное представление в орган финансовой разведки информации и документов, а также сообщений об операциях (сделках), подлежащих контролю и сообщению;

3. ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ (KYC) И ОЦЕНКА РИСКОВ

3.1. При регистрации и обслуживании клиентов Компании строго соблюдаются требования KYC, что предполагает сбор и проверку исчерпывающих данных, необходимых для идентификации личности. Клиент обязан предоставить полное имя, дату рождения, гражданство, а также документ, удостоверяющий личность (паспорт или иной документ с указанием номера, серии, даты выдачи и подтвержденный фотографией), дополненный актуальным адресом проживания и контактной информацией. Помимо этого, запрашиваются сведения о роде деятельности клиента и источниках происхождения его средств. Эти меры соответствуют как международным стандартам, в том числе рекомендациям FATF, так и требованиям национального законодательства, регулируемого Законом Кыргызской Республики от 6 августа 2018 года №87 «О противодействии легализации (отмыванию) преступных доходов и финансированию терроризма».

3.2. Компания проверяет подлинность предоставленных документов и сведений. Используются передовые методы подтверждения личности, включая проверку паспортных данных через государственные базы (при возможности), а также биометрическую идентификацию. Компания не предоставляет доступ к сервисам до тех пор, пока личность клиента не будет успешно подтверждена в рамках процедуры Customer Identification Program (CIP) .

3.3. После завершения KYC-процедур Компания осуществляет оценку рисков, связанных с каждым клиентом, и относит его к определенной категории риска (низкий, средний, высокий). Критерии оценки включают результаты проверки санкционных списков и списков нежелательных лиц, статус клиента, страну проживания и регистрации бизнеса, цель использования криптосервиса, а также объемы предполагаемых операций. На основании этих факторов вырабатывается риск-профиль клиента. Клиенты с повышенным уровнем риска подвергаются усиленной проверке. Для них проводится расширенная процедура Due Diligence (EDD): запрашиваются дополнительные документы (подтверждение адреса, финансовые выписки, сведения о бенефициарах и т.д.) и руководством компании дается разрешение на обслуживание такого клиента. Данная риск-ориентированная методология соответствует передовым практикам международных финансовых институтов и позволяет применять к каждому клиенту индивидуальные меры контроля.

3.4. **Работа с PEP (политически значимыми лицами) / Handling PEP (Politically Exposed Persons)**

1) Компания придает повышенное значение выявлению политически значимых лиц (Politically Exposed Persons, PEP) среди своих клиентов. В процессе KYC каждый клиент в анкете указывает, является ли он сам или ближайшие члены его семьи/связанные лица политически значимыми (например, занимают ли государственные должности). Кроме самодекларации, компания самостоятельно проводит проверку по специализированным базам данных PEP, которые содержат сведения о мировых политических деятелях, чиновниках и их родственниках. Такой двойной подход обеспечивает надежность идентификации: даже если клиент не раскрыл статус ПЭП, система может обнаружить его по внешним источникам. В случае выявления информация об этом фиксируется в профиле клиента, и ему присваивается соответствующий статус риска (высокий).
2) Клиенты, отнесенные к категории PEP, автоматически подпадают под расширенные процедуры проверки. Компания проводит углубленный Due Diligence в отношении политически значимых лиц. В рамках EDD запрашиваются дополнительные сведения и документы, подтверждающие благонадежность клиента и законность происхождения его средств. Например, компания может потребовать предоставить декларацию о доходах или выписку с банковских счетов, подтверждающую уровень доходов, сопоставимый с проводимыми операциями. Также могут быть затребованы рекомендации от обслуживающего банка или иного финансового учреждения. Цель данных мер – убедиться, что средства ПЭП не связаны с коррупцией, взятками или другими злоупотреблениями служебным положением. Все собранные материалы анализируются отделом комплаенса, и решение о продолжении обслуживания такого клиента принимается на уровне руководства компании.
3) Операции и счета клиентов-PEP находятся под усиленным контролем. Для таких клиентов

устанавливаются пониженные пороги для отметки транзакций как крупные или необычные. Любая транзакция, проводимая PEP либо по счету, принадлежащему PEP, оценивается на предмет соответствия профилю – суммы транзакций соотносятся с известным уровнем доходов, проверяется назначение платежей. Компания применяет принцип «four-eyes» (двойной контроль) для операций PEP: помимо автоматических алгоритмов мониторинга, каждую крупную или нестандартную транзакцию вручную проверяет сотрудник комплаенса. Если операция вызывает вопросы, от клиента могут потребовать пояснения и документы. В случае серьезных подозрений транзакция приостанавливается и инициируется процедура SAR.

4) Заведение клиента, являющегося PEP, или продолжение обслуживания такого клиента требует одобрения высшего руководства Компании. Информация о наличии политически значимых клиентов отражается во внутренних отчетах и доводится до сведения руководителя службы комплаенса и директоров компании. Ежегодно проводится пересмотр статуса PEP. Все сведения о клиентах-PEP хранятся с особо высоким уровнем конфиденциальности. В случае запросов от регуляторов или финансовой разведки, касающихся операций PEP, Компания предоставляет всю запрошенную информацию.

3.6 **Идентификация бенефициарных владельцев (UBO)**

1) В соответствии с международными стандартами и законодательством КР, Компания в обязательном порядке устанавливает личность бенефициарных владельцев (Ultimate Beneficial Owners, UBO) своих клиентов — юридических лиц. Бенефициарным владельцем признается физическое лицо, которое в итоге прямо или косвенно (через третьих лиц или цепочку компаний) владеет правом собственности более 25% уставного капитала клиента либо контролирует его действия иным образом. Процедура идентификации направлена на то, чтобы исключить использование номинальных лиц для сокрытия реальных выгодоприобретателей.
2) При установлении деловых отношений Клиент обязан раскрыть структуру собственности компании вплоть до конечных физических лиц. Для верификации личности бенефициара Компания запрашивает документы, аналогичные тем, что требуются для физических лиц (паспорт, подтверждение адреса), а также документы, подтверждающие долю владения. В случаях, когда структура собственности является сложной или многоуровневой, от Клиента требуется предоставить документальное подтверждение всех звеньев цепочки владения. Если бенефициарный владелец не может быть выявлен или существуют сомнения в достоверности сведений, бенефициаром признается физическое лицо, осуществляющее высшее руководство клиентом (принимающее стратегические решения).
3) Сведения о бенефициарных владельцах подвергаются тщательной проверке. Все выявленные UBO проверяются по санкционным спискам, спискам террористов/экстремистов и базам данных PEP. Если бенефициар компании является политически значимым лицом (PEP) или резидентом высокорискованной юрисдикции, к самому Клиенту-юридическому лицу автоматически применяются меры усиленной проверки (Enhanced Due Diligence).

3.7 Санкционные списки и проверки / Sanctions Lists and Screening

1) Компания строго соблюдает санкционные режимы и проводит проверку клиентов по международным спискам санкций. В ходе KYC-онбординга каждый новый клиент проходит

скрининг по актуальным санкционным спискам. Также учитываются национальные списки, если таковые предусмотрены регуляторами. Для автоматизации этой проверки применяются специализированные системы, которые сверяют персональные данные клиента (ФИО, дату рождения, гражданство) с записями в указанных базах данных. Данный процесс позволяет на этапе приема клиента убедиться в отсутствии у него санкционного статуса либо принадлежности к санкционированным организациям.

2) Санкционный комплаенс носит непрерывный характер. База клиентов Компании регулярно (не реже одного раза в день) сверяется с обновлениями санкционных списков. В случае, если действующий клиент в ходе обслуживания попадает под санкции, система сигнализирует об этом событии. Компания немедленно принимает необходимые меры: приостанавливает операции по счетам такого клиента, блокирует возможность вывода средств и проводит дополнительное расследование. О выявлении санкционного лица среди клиентов информируются регулятор. Дальнейшие действия предпринимаются в соответствии с указаниями закона и регуляторов.

4. МОНИТОРИНГ ТРАНЗАКЦИЙ И ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

4.1. Компания реализует мониторинг всех транзакций клиентов. Для этих целей используется специализированная AML-платформа, обеспечивающая анализ блокчейн-операций на соответствие критериям рисков. Система автоматически отслеживает движение средств на криптовалютных кошельках, связанных с платформой, и сопоставляет транзакции с известными шаблонами и базами данных. Мониторинг охватывает все основные криптоактивы, поддерживаемые на платформе, включая токены стандарта ERC-20 и другие цифровые активы.

4.2. Система проводит оценку каждой транзакции по ряду показателей риска. Система учитывает объем перевода, частоту и последовательность операций, связанные адреса кошельков и географические факторы. Транзакции, существенно отклоняющиеся от обычного поведения клиента (нестандартно крупные суммы, необычное направление переводов), либо разбитые на множество мелких операций вызывают подозрение. Также отмечаются операции, связанные с анонимизирующими сервисами или ведущие в юрисдикции с высоким уровнем риска. Система присваивает каждой транзакции или адресу риск-оценку на основании исторических данных и известных связей адреса, включая возможные связи с даркнет-площадками или кошельками, замешанными в ранее выявленных незаконных схемах. Если транзакция превышает заданные пороговые значения риска или отвечает нескольким подозрительным критериям, система помечает ее для дополнительной проверки. Таким образом, на основе автоматизированного анализа формируется перечень триггеров подозрительных транзакций.

4.3. Технология мониторинга интегрирована с базами данных санкций и нежелательных субъектов. Все транзакции проверяются на предмет участия санкционированных лиц или организаций. Система автоматически сверяет адреса, задействованные в переводе, с адресами из мировых санкционных списков (ООН, OFAC, ЕС и др.). Если выявляется совпадение, такая транзакция немедленно получает отметку “подозрительная”. Аналогично, транзакции, в которых участвуют адреса, ранее идентифицированные как принадлежащие террористическим группам или другим запрещенным организациям, получают высокий риск-скоринг.

4.4. Все транзакции, помеченные системой как подозрительные, подвергаются углубленной проверке со стороны отдела комплаенса. Специалисты анализируют детали операции, сопоставляют их с профилем клиента и иными доступными сведениями. При необходимости запрашивается дополнительная информация у клиента (обоснование экономического смысла транзакции, подтверждающие документы по происхождению средств). На время расследования транзакция может быть приостановлена (временно заморожена на уровне платформы) до выяснения всех обстоятельств. Если по результатам проверки подозрения не подтверждаются, операция разблокируется и проводится. В случае же, когда сомнения усиливаются, запускается процедура подготовки отчета о подозрительной активности. Такой многоуровневый подход (автоматическое выявление + ручная проверка) обеспечивает высокий уровень AML-контроля на платформе.

5. ХРАНЕНИЕ СВЕДЕНИЙ И ДОКУМЕНТОВ

5.1 Компания уделяет особое внимание безопасному хранению и защите данных, собранных в рамках KYC и мониторинга. Вся клиентская информация (копии документов, анкеты, адреса, записи коммуникаций) и данные о транзакциях сохраняются в защищенной базе данных. Доступ к ней строго ограничен кругом уполномоченных сотрудников отдела комплаенса и безопасности. Для хранения используются серверы, отвечающие требованиям к кибербезопасности, с применением шифрования данных. Согласно требованиям законодательства, сведения о клиентах и проведенных ими операциях хранятся не менее 5 лет с момента окончания отношений с клиентом (либо дольше, если это предписано локальными нормами). Такая длительность хранения обеспечивает возможность ретроспективного анализа и проверки по запросам регуляторов или правоохранительных органов. Кроме того, журнал транзакций и отчеты (SAR) также хранятся в течение установленного срока. Компания получила от клиентов необходимые согласия на обработку и хранение персональных данных, соблюдая Закон КР о защите персональных данных. Внутренние политики предписывают регулярное резервное копирование данных и меры по предотвращению их утечки. Данные хранятся и обрабатываются преимущественно на территории Кыргызской Республики, в соответствии с требованием размещения серверов локально (для обеспечения юрисдикционного контроля над информацией). Благодаря этим мерам Амана обеспечивает как выполнение нормативных требований по хранению, так и сохранность конфиденциальной информации клиентов.

6. ВЗАИМОДЕЙСТВИЕ С ГОСУДАРСТВЕННЫМИ ОРГАНАМИ И ОТЧЕТНОСТЬ О ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ (SAR)

6.1 При выявлении транзакции или деятельности, вызывающей подозрения в отношении легальности источника средств или цели операции, Компания готовит специальный отчет – Отчет о подозрительной активности (Suspicious Activity Report, SAR). Ответственный сотрудник по финансовому мониторингу (AML-офицер) фиксирует в отчете все относящиеся к делу детали: данные клиента, описание активности, причины, по которым она классифицирована как подозрительная (с указанием конкретных критериев или индикаторов), а также принятые внутренние меры (например, приостановка транзакции). Отчет проходит внутреннее согласование руководителем отдела комплаенса и юридическим отделом при необходимости, после чего подлежит передаче в компетентные органы, а именно Государственная служба финансовой разведки при Министерстве финансов Кыргызской Республики.

6.2 В соответствии с требованиями законодательства Кыргызской Республики, информация о подозрительной активности должна быть своевременно направлена в государственные органы, осуществляющие финансовый мониторинг. Компания направляет подготовленный SAR в Государственную службу финансовой разведки (ГСФР) при Кабинете Министров КР, которая выступает финансовой разведкой (FIU) Кыргызской Республики. Одновременно, при необходимости, уведомляется отраслевой регулятор криптообменников – Государственная служба регулирования и надзора за финансовым рынком (Госфиннадзор) при Министерстве

экономики и финансов. Отчет о подозрительной операции направляется незамедлительно после его подготовки, в пределах сроков, установленных законодательством.

6.3 Помимо индивидуальных сообщений о подозрительных транзакциях, Компания выполняет обязательства по регулярной отчетности перед регуляторами. Компания готовит и подает предусмотренные законом периодические отчеты – например, отчеты о выполнении внутренних правил ПОД/ФТ, количество проведенных KYC-процедур, статистику выявленных подозрительных случаев. Такие отчеты направляются в Госфиннадзор по установленному графику, согласно нормативным актам). Также по запросу государственных органов предоставляются разовые отчеты или разъяснения. Компания ведет полный учет всех поданных сообщений о подозрительной активности (реестр SAR) и действий, предпринятых в отношении таких случаев. При поступлении запросов от правоохранительных органов или финансовой разведки Компания оперативно предоставляет необходимые данные в рамках сотрудничества. Все сотрудники, задействованные в процессе отчетности, обеспечивают конфиденциальность передаваемой информации и соблюдение законодательства о персональных данных.

6.4 В компании назначено должностное лицо, ответственное за соблюдение требований ПОД/ФТ (AML Compliance Officer). Этот специалист обеспечивает выполнение программы AML внутри организации и служит точкой контакта для связи с государственными органами (Госфиннадзор, Государственная служба финансовой разведки). Компания готова к плановым и внеплановым проверкам со стороны регуляторов. Компания предоставляет полный доступ к необходимой документации и отчетности для надзорных органов. Периодически проводятся внутренние аудиты и стресс-тесты AML-системы, результаты которых могут представляться регулятору по требованию. В случае выявления недостатков или нарушений компания оперативно уведомляет об этом регуляторов и предпринимает корректирующие меры. Такой подход обеспечивает прозрачность деятельности Амана перед государством и укрепляет доверие со стороны надзорных органов.

6.5 С учетом особенностей регулирования виртуальных активов в Кыргызской Республике Компания соблюдает дополнительные нормативы, введенные для криптоиндустрии. В частности, компания выполняет правило путешествия (Travel Rule), требуемое локальными положениями и рекомендациями FATF: при криптовалютных транзакциях на сумму свыше 85 000 сомов (около 1 000 USD), Компания собирает и передает необходимую идентификационную информацию о отправителе и получателе перевода соответствующим провайдерам или компетентным органам. Это включает имя отправителя, номер его аккаунта/кошелька, данные получателя и идентификаторы транзакции – такие сведения сопровождают перевод и позволяют отслеживать его на предмет противодействия отмыванию денег. Кроме того, Компания соблюдает установленные пороги финансового мониторинга: крупные операции (свыше установленных сумм) отражаются в обязательной отчетности перед регуляторами, даже если они не признаны подозрительными. Компания также учитывает требования налогового законодательства (декларирование доходов от криптоопераций, содействие налоговым органам в случае запросов по операциям клиентов) и другие обязательства перед государством. Соблюдение всех перечисленных норм является неотъемлемой частью деятельности Компании и контролируется на уровне руководства.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1 Настоящие Правила подлежит изменению в случае изменения законодательства Кыргызской Республики.

7.2 Вопросы, не урегулированные настоящими Правилами, регулируются действующим законодательством Кыргызской Республики, международной практикой и внутренними документами Компании.

7.3 Если в результате изменения законодательства или нормативных актов Кыргызской Республики, отдельные статьи настоящих Правил вступают в противоречие с ними, эти статьи утрачивают силу, и до момента внесения изменений в настоящие Правила.

7.4 Настоящие Правила вступает в силу с момента его утверждения Директором Компании.