УТВЕРЖДЕНО
Приказом Генерального Директора
ОсОО «ФинКИТ.про»
№14 от «29» сентября 2026 г.

ПОЛИТИКА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ

ЦЕЛЬ ДОКУМЕНТА

- Соблюдение законодательства Кыргызской Республики и международных стандартов AML/CFT;
- Предотвращение использования платформы в целях отмывания доходов, финансирования терроризма и иных незаконных операций;
- Выполнение требований по идентификации клиентов (KYC);
- Мониторинг транзакций и источников средств (KYT, SoF, SoW, SoA).

ОБЩИЕ ПРИНЦИПЫ

- ОсОО «ФинКИТ.про» применяет риск-ориентированный подход (Risk-Based Approach).
- Политика применяется ко всем клиентам и операциям.
- Настоящая Политика обязательна к исполнению всеми сотрудниками, подрядчиками и клиентами ОсОО «ФинКИТ.про».

1. ИДЕНТИФИКАЦИЯ КЛИЕНТОВ (KYC)

1.1. Клиент предоставляет:

- ФИО, дату рождения, гражданство;
- паспортные данные (документ, удостоверяющий личность);
- адрес проживания и/или регистрации;
- фото/видео-селфи для подтверждения личности;
- контактные данные: телефон, email.

1.2. Дополнительно:

- utility bill, банковская выписка (подтверждение адреса);
- при необходимости — подтверждение статуса налогового резидента.

1.3. Для корпоративных клиентов (KYB):

- учредительные документы;
- реестры участников/акционеров;
- идентификация бенефициаров;
- лицензии (если применимо).

2. ИСТОЧНИК ПРОИСХОЖДЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Компания может запросить:

- подтверждение происхождения средств (договоры, справки, выписки);
- обоснование накопленного капитала (продажа активов, наследство и т.п.);
- подтверждение происхождения актива (договоры, справки, выписки);
- заявления или пояснительные письма клиента.

3. МОНИТОРИНГ ТРАНЗАКЦИЙ (KYT)

3.1. Все транзакции подлежат автоматическому мониторингу и фильтрации по:

- юрисдикциям (санкционные, офшорные);
- объёмам и частоте операций;
- используемым валютам и криптоактивам;
- профилю риска клиента.

3.2. Используются внешние или внутренние программные решения (собственный софт или сторонние провайдеры), обеспечивающие оценку рисков и соответствие стандартам.

3.3. Подозрительные транзакции блокируются и передаются в соответствующие органы, если это требуется законом.

4. ОТКАЗ В ОБСЛУЖИВАНИИ

Компания оставляет за собой право отказать в открытии счёта или прекратить обслуживание:

- при наличии подозрений в незаконной деятельности;
- при отказе клиента предоставлять требуемую информацию;
- при несоответствии требованиям юрисдикции.

5. ХРАНЕНИЕ И ОТЧЁТНОСТЬ

- Все данные хранятся не менее 5 лет с момента завершения отношений.
- Вся документация архивируется в соответствии с законодательством КР.
- Запросы регуляторов исполняются в установленные сроки.

6. ПОДОЗРИТЕЛЬНЫЕ СИТУАЦИИ

Примеры ситуаций:

- клиент избегает KYC или предоставляет поддельные документы;
- необоснованные суммы транзакций;
- использование сложных схем, множественные переводы;
- расхождения между профилем и транзакциями.

7. ОБНОВЛЕНИЕ И АУДИТ

- Политика пересматривается не реже 1 раза в год.
- Ответственные сотрудники назначаются приказом.
- Проводится регулярная проверка соответствия внутренним регламентам.