ПОЛИТИКА

Политика идентификации и проверки клиентов (KYC / KYB)

Know Your Customer / Know Your Business Policy

Компания	Free Bird PSP L.L.C-FZ
Код документа	[03-000]
Версия	1.1
Дата утверждения	06.10.2026
Владелец документа	MLRO
Периодичность пересмотра	Ежегодно или при изменении законодательства / процедур
Классификация	Конфиденциально (Confidential)
Контакты	ceo.freebird@gmail.com

Дубай · 2026

ОРГАНИЗАЦИОННАЯ МОДЕЛЬ И СОВМЕЩЕНИЕ ФУНКЦИЙ

На дату утверждения настоящего документа функции всех ролей, упомянутых в документе, — Директора (CEO), MLRO (Money Laundering Reporting Officer), Compliance Lead, Risk Committee, ответственного лица за защиту персональных данных, Support Team и Technical Lead — исполняет единолично Директор Компании Кузнецов Роман Игоревич, назначенный Решением единственного участника № 2. Все ссылки в документе на указанные роли и органы следует читать как ссылки на Директора Компании.

При совмещении функций одним лицом применяются следующие правила:

— многоуровневая эскалация (Support → Compliance → MLRO → Risk Committee → CEO) выполняется путём последовательного документирования решения на каждом уровне в журнале эскалаций с указанием оснований; решения без письменного обоснования не допускаются;

— решения, отнесённые к компетенции Risk Committee, оформляются письменным решением Директора с приложением материалов проверки;

— для компенсации отсутствия принципа «четырёх глаз» все решения о принятии High-Risk клиентов, отказах, разблокировке средств, подаче STR/SAR и исключениях из политик фиксируются в журнале, а не реже одного раза в год система AML/CFT проверяется независимым внешним консультантом (аудитором);

— Компания вправе привлечь внешнего MLRO / Compliance-специалиста на условиях аутсорсинга и назначает отдельных лиц на роли MLRO и Compliance Lead по мере роста штата и оборотов, а также по требованию Банков-партнёров, регуляторов или применимого законодательства. Такое назначение оформляется решением Директора и не требует пересмотра документа.

1. Цель и область применения

Настоящая политика определяет процедуры проверки клиентов (KYC — физические лица, KYB — юридические лица), а также стандарты Customer Due Diligence (CDD) и Enhanced Due Diligence (EDD), применяемые Free Bird PSP L.L.C-FZ в целях идентификации клиентов, подтверждения право- и дееспособности, предотвращения мошенничества, выполнения AML/CFT требований, обеспечения прозрачности происхождения средств и защиты платёжной системы и банков-партнёров.

2. Кто проходит KYC / KYB

KYB обязателен для всех мерчантов — юридических лиц. KYC проводится в отношении физических лиц, связанных с мерчантом: UBO (25% и более), директоров, лиц с правом подписи и представителей. Покупатели (плательщики по СБП) не являются клиентами Компании и KYC не проходят — их идентифицируют банки плательщиков (AML Policy, раздел 6).

3. Документы для KYC (физические лица)

Действующий паспорт / ID; дата и место рождения, гражданство; подтверждение адреса проживания (не старше 3 месяцев); селфи / проверка «живого присутствия» (liveness) при дистанционной идентификации; для UBO и клиентов High Risk — сведения об источнике средств и благосостояния.

4. Документы для KYB (юридические лица)

Свидетельство о регистрации или выписка из реестра (не старше 3 месяцев); устав (MoA/AoA); реестр участников и директоров; схема структуры владения до конечного бенефициара; декларация UBO; документ о полномочиях подписанта; подтверждение юридического и фактического адреса; лицензии (если деятельность лицензируется); сайт или приложение с публичной офертой, политикой возврата и контактами; описание бизнес-модели; ожидаемые обороты, средний чек и география покупателей; для Medium/High Risk — финансовая отчётность или банковская выписка за последние 3 месяца.

Бенефициарным владельцем (UBO) признаётся физическое лицо, прямо или косвенно владеющее 25% и более капитала либо голосующих акций (долей) компании, либо иным образом осуществляющее контроль над её деятельностью. При отсутствии лица, соответствующего данному критерию, UBO считается лицо, занимающее должность единоличного исполнительного органа (руководителя) компании.

Для мерчантов, получающих расчёты в USDT (раздел 17a AML Policy), дополнительно запрашиваются: адрес кошелька и сеть (TRC-20 / BEP-20); подтверждение принадлежности кошелька мерчанту (тестовая транзакция или подпись сообщения закрытым ключом); результаты блокчейн-скрининга адреса (KYT). Выплаты на адреса, не прошедшие проверку или не включённые в белый список, не проводятся.

Периодический пересмотр (KYB refresh): High Risk — раз в 12 месяцев, Medium Risk — раз в 2 года, Low Risk — раз в 3 года, а также внепланово при истечении срока действия документов, смене UBO, директора или реквизитов, срабатывании триггеров мониторинга.

5. Customer Due Diligence (CDD)

Идентификация, санкционный скрининг, оценка бизнес-модели и соответствия транзакций заявленной деятельности.

6. Enhanced Due Diligence (EDD)

Применяется при: high-risk юрисдикциях и отраслях, резких скачках оборотов, отсутствии подтверждённой бизнес-модели, отрицательном новостном фоне. Включает интервью, подтверждение источников средств, запрос договоров, анализ транзакций.

Для PEP, членов их семей и близких лиц (RCA) EDD обязателен; решение об установлении отношений принимает Директор (senior management approval). Агентства недвижимости и обменные / финансовые сервисы относятся к категории High Risk и подключаются только после EDD.

7. High-Risk Industries

Включает крипто-миксеры, беттинг без лицензии, серые финансовые услуги, Forex без регулятора, дропшиппинг высокой интенсивности, adult-контент, подакцизные товары без лицензий.

8. Запрещённые виды деятельности

Мошенничество, обналичивание, даркнет, незаконный криптобизнес, оружие, наркотики, схемы обхода санкций, финансовые пирамиды, операции без экономического смысла.

9. Постоянный мониторинг

Непрерывный мониторинг транзакций: происхождение средств, аномалии, IP-риски, юрисдикции, попытки дробления операций.

10. Red Flags

Несоответствие транзакций заявленному бизнесу, уклонение от проверки, офшоры без операционной деятельности, резкие изменения профиля, новые реквизиты, ночная активность, использование TOR/VPN.

11. Хранение данных

Категория	Срок хранения
KYC	не менее 5 лет
Транзакции	не менее 5 лет
Логи	12 месяцев
EDD	5–7 лет

12. Обучение

Ежегодное обучение AML/KYC, тестирование сотрудников, внутренние проверки.

13. Ответственность

Отказ в обслуживании, блокировка, отчёты регуляторам при нарушениях или предоставлении ложных данных.

14. Обновление политики

Обновление ежегодно либо при изменении законодательства или внутренних процедур.

15. Операционный процесс KYC/KYB

Процесс онбординга и проверки клиентов осуществляется в следующем порядке:

Шаг 1. Первичный скрининг

- сбор базовой информации о клиенте;
- предварительная оценка риска (юрисдикция, тип бизнеса);
- первичный санкционный скрининг.

Шаг 2. Сбор документов

- получение полного пакета KYC/KYB документов;
- проверка полноты и корректности.

Шаг 3. Верификация личности и бизнеса

- проверка личности (для физических лиц);
- проверка регистрации и юридического статуса компании;
- идентификация и верификация конечных бенефициаров (UBO).

Шаг 4. Санкционный и PEP-скрининг

- проверка по спискам: UN, OFAC, EC, Великобритания, а также по локальному перечню террористических организаций и лиц ОАЭ (Cabinet Decision No. 74/2020);
- проверка на PEP, а также на членов семьи и известных близких связанных лиц PEP (Relatives and Close Associates, RCA), и негативный новостной фон (adverse media).

Шаг 5. Оценка риска

- присвоение категории риска (Low / Medium / High) по количественной модели Risk Scoring & Acceptance Policy;
- сопоставление с моделью риск-скоринга (0–100 баллов).

Шаг 6. Принятие решения

- одобрение;
- запрос дополнительной информации;

- перевод на EDD;
- отказ.

Шаг 7. Активация

- активация клиента в системе;
- установка лимитов.

Шаг 8. Последующий мониторинг

- постоянный контроль транзакций;
- пересмотр риска при срабатывании триггеров.

Все этапы фиксируются и подлежат аудиту.

16. Правила принятия решений (Risk-Based Logic)

- отсутствие или невозможность верификации UBO → приостановка онбординга;
- высокорисковая юрисдикция (серый/чёрный список FATF) → обязательный EDD;
- номинальная структура без прозрачности → отказ или эскалация;
- отсутствие признаков реальной деятельности → отказ;
- несоответствие бизнес-модели транзакциям → эскалация;
- негативный новостной фон или санкции → эскалация на уровень MLRO.

Все решения документируются с обоснованием.

17. Используемые технологии и инструменты

Free Bird PSP L.L.C-FZ использует комбинацию автоматизированных и ручных инструментов для KYC/KYB и AML, включая:

- системы санкционного скрининга;
- системы мониторинга транзакций;
- внутренние модели риск-скоринга.

Для всех клиентов со средним и высоким уровнем риска применяется обязательная ручная проверка.

18. Процедура эскалации

Подозрительные и высокорисковые кейсы рассматриваются по единой схеме (согласовано с AML Policy и Risk Scoring & Acceptance Policy):

1. Уровень 1 — Support
2. Уровень 2 — Compliance
3. Уровень 3 — MLRO
4. Уровень 4 — Risk Committee
5. Уровень 5 — CEO

Эскалация обязательна в случаях: совпадения по санкционным спискам; подозрительных транзакционных паттернов; высокого уровня риска (60+ баллов); неполных или противоречивых данных.

Все случаи эскалации фиксируются.

19. Критерии отказа в обслуживании

- невозможность верифицировать личность или структуру владения;
- участие в запрещённых видах деятельности;
- предоставление ложной или вводящей в заблуждение информации;
- попытки обхода процедур KYC/KYB;
- наличие санкционных ограничений.

Free Bird PSP L.L.C-FZ оставляет за собой право отказать в обслуживании без раскрытия подробных причин.