

RISK MANAGEMENT POLICY

Mercury Pro / ОсОО «Меркури Про»

Последнее обновление: февраль 2026

1. ЦЕЛЬ ПОЛИТИКИ

Настоящая политика устанавливает систему управления рисками Mercury Pro. Она направлена на предотвращение финансовых, операционных, юридических, регуляторных, технологических и репутационных рисков, связанных с деятельностью компании и обслуживанием клиентов.

2. ПРИНЦИПЫ УПРАВЛЕНИЯ РИСКАМИ

- системность и непрерывность;
- прозрачность процессов;
- приоритет превентивных мер;
- персональная ответственность;
- документирование всех действий;
- соблюдение законодательства и требований банков-партнёров.

3. КАТЕГОРИИ РИСКОВ

3.1. *Операционные риски*

Ошибки сотрудников, сбои процессов, некорректные таблицы, неверные расчёты, нарушения процедур, человеческий фактор.

3.2. *Финансовые риски*

Кассовые разрывы, задержки выплат, просадки у партнёров, зависание транзакций, волатильность курса.

3.3. *AML/KYC/KYB риски*

Недостаточная идентификация клиентов, обслуживание запрещённых отраслей, пропуск мошеннических схем.

3.4. *Юридические риски*

Несоответствие договорам, нарушение ПОД/ФТ, ошибки в документации, ответственность за действия клиента.

3.5. *Регуляторные риски*

Изменение законодательства, новые правила ПВТ, ограничения банков, изменения санкционных режимов.

3.6. *Технологические риски*

Взлом, утечки данных, потеря доступа, сбои API, зависимость от внешних сервисов.

3.7. *Репутационные риски*

Отрицательные новости, жалобы клиентов, ошибки работы, связь с незаконной деятельностью.

4. МЕТОДОЛОГИЯ ОЦЕНКИ РИСКОВ

Каждый риск оценивается по двум шкалам:

- Вероятность: Low / Medium / High
- Влияние: Low / Medium / High

Используется матрица оценки риска. Риски с уровнем High подлежат немедленной эскалации.

5. КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ (RISK CONTROLS)

- двойные проверки данных в таблицах;
- утверждение лимитов;
- обязательные KYC/KYB процедуры;
- использование санкционного скрининга;
- логирование всех действий;
- контроль доступа сотрудников;
- резервные каналы связи и выплат;
- регулярный аудит процессов.

6. МОНИТОРИНГ РИСКОВ

- ежедневный контроль транзакций;
- анализ аномалий (суммы, частоты, юрисдикции);
- проверка IP-рисков и VPN;
- еженедельный отчёт операционного отдела;
- ежемесячный комплаенс-отчёт собственнику;
- фиксация всех отклонений.

7. МЕРЫ СНИЖЕНИЯ РИСКОВ (RISK MITIGATION)

- заморозка транзакций до разъяснений;
- перевод клиента в риск-категорию High;
- применение EDD;
- запрос подтверждения источника средств;
- снижение лимитов;
- временная приостановка обслуживания;
- отказ в обслуживании.

8. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ (INCIDENT MANAGEMENT)

Порядок действий:

- 1) фиксация события в журнале инцидентов;
- 2) немедленное уведомление AML Officer / собственнику;
- 3) анализ первопричины;
- 4) блокировка опасных операций;
- 5) подготовка внутреннего отчёта;
- 6) устранение последствий;
- 7) внедрение мер предотвращения повторения.

9. REPORTING / ОТЧЁТНОСТЬ

- внутренние отчёты по инцидентам;
- отчёт собственнику;
- отчёты банкам-партнёрам при запросах;
- предоставление данных государственным органам по закону.

10. ОБЯЗАННОСТИ УЧАСТНИКОВ

Compliance Officer:

- оценка рисков;
- анализ транзакций;
- утверждение EDD;
- эскалация инцидентов.

Операционный отдел:

- выполнение процедур;
- корректность данных;
- ведение журналов;
- первичный мониторинг.

Руководство:

- утверждение политики;
- распределение ресурсов;
- принятие решений при High-risk ситуациях.

11. ОБНОВЛЕНИЕ ПОЛИТИКИ

Политика пересматривается:

- ежегодно;
- при изменении законодательства;
- при запуске новых продуктов;
- после серьёзных инцидентов.

Контакты:

ОcOO «Меркури Про», Бишкек, пр. Манаса, д.40, 2 эт., 206 каб.
Email: info@mercury-pro.com