AML RISK FRAMEWORK

PROJEKT BEE COIN TOKEN

AML RISK FRAMEWORK

Bee Coin – Risk-Based Compliance Model

Wersja: 1.0
Data obowiązywania: 26.02.2026.
Administrator: PartnerLedger OÜ (Estonia)

1. Cel dokumentu

Niniejszy dokument opisuje podejście do zarządzania ryzykiem związanym z nadużyciami oraz bezpieczeństwem infrastruktury technologicznej projektu Bee Coin.

Framework ma charakter informacyjny i przedstawia ogólne standardy bezpieczeństwa stosowane w projekcie.

Dokument nie stanowi deklaracji prowadzenia działalności regulowanej w zakresie usług finansowych.

2. Model podejścia do ryzyka (Risk-Based Approach)

Administrator stosuje podejście oparte na analizie ryzyka, które polega na:

- identyfikacji potencjalnych zagrożeń,
- ocenie poziomu ryzyka operacyjnego,
- wdrażaniu adekwatnych środków bezpieczeństwa.

Zakres działań może być dostosowywany w zależności od charakteru interakcji użytkownika z ekosystemem.

3. Kategorie ryzyka

Ryzyko jurysdykcyjne

Ocena krajów o podwyższonym ryzyku regulacyjnym lub sankcyjnym.

Ryzyko operacyjne

Nietypowe wzorce aktywności w infrastrukturze technologicznej.

Ryzyko reputacyjne

Działania mogące naruszać zasady bezpieczeństwa ekosystemu.

Ryzyko technologiczne

Wykorzystanie narzędzi automatycznych lub prób obejścia zabezpieczeń.

4. Screening i monitoring

Administrator może stosować środki techniczne, takie jak:

- automatyczna analiza ryzyka interakcji,
- sprawdzanie zgodności z listami sankcyjnymi dostępnymi publicznie,
- monitoring zdarzeń o podwyższonym ryzyku.

Działania te mają charakter prewencyjny i technologiczny.

5. Weryfikacja użytkownika (KYC Layer)

W zależności od poziomu ryzyka, dostęp do wybranych funkcji może wymagać dodatkowej weryfikacji tożsamości.

Proces ten może obejmować:

- potwierdzenie tożsamości,
- analizę rezydencji użytkownika,
- dodatkową ocenę bezpieczeństwa.

Szczegóły znajdują się w Polityce KYC/AML.

6. Zarządzanie dostępem

Administrator może:

- ograniczyć funkcjonalność,
- zawiesić dostęp,
- odmówić korzystania z określonych narzędzi

w przypadku wykrycia podwyższonego ryzyka.

7. Współpraca z dostawcami zewnętrznymi

W zakresie analizy ryzyka Administrator może korzystać z usług podmiotów trzecich oferujących:

- narzędzia weryfikacyjne,
- monitoring blockchain,

- systemy analityczne.

Dostawcy działają zgodnie z zasadami GDPR.

8. Brak charakteru usług AML w rozumieniu finansowym

Niniejszy framework nie oznacza, że Administrator działa jako instytucja obowiązana w rozumieniu przepisów o przeciwdziałaniu praniu pieniędzy.

Działania mają charakter operacyjny i służą bezpieczeństwu infrastruktury technologicznej.

9. Jurisdiction Risk Matrix (ogólne podejście)

Administrator może stosować klasyfikację jurysdykcji według poziomu ryzyka:

- niskie ryzyko – standardowy dostęp,
- podwyższone ryzyko – dodatkowa weryfikacja,
- wysokie ryzyko – ograniczenie funkcjonalności.

Szczegółowe kryteria nie są publicznie ujawniane.

10. Aktualizacje frameworku

Framework może być aktualizowany wraz ze zmianami regulacyjnymi, technologicznymi lub operacyjnymi.

Aktualna wersja publikowana jest w Serwisie dostępnym pod adresem:

https://beecointoken.com („Serwis”).