Nexus Capital — AML / CFT Policy

Nexus Capital Ltda. - Tax ID (CNPJ) 65.737.320/0001-74 - Florianópolis/SC - Brazil

Update: 2026-04-20

Official contact: meajuda@nexuscapitalp2p.com.br - WhatsApp as indicated on the website.

This document is published for transparency. Internal operational procedures are confidential to preserve the effectiveness of controls.

1. Purpose and institutional posture

Nexus Capital proactively adopts the regulated standard for the prevention of money laundering (AML) and counter financing of terrorism (CFT), even where the formal classification of virtual asset service providers is still being defined under Brazilian law. We operate as a P2P merchant under the rules of the platforms used and align with the requirements of the Central Bank of Brazil, COAF (Brazil's FIU) and applicable legal framework.

2. Scope

This policy applies to every counterparty trading with Nexus Capital, to all staff and to vendors involved in AML/CFT-sensitive activities, on any P2P platform on which we operate.

3. Legal basis

- Law No. 9,613/1998 — Brazilian AML/CFT Act.
- Law No. 14,478/2022 — Brazilian Virtual Assets Legal Framework.
- COAF Resolution No. 36/2021 and related Circulars.
- Central Bank of Brazil rules applicable to virtual asset service provision (current BCB Resolutions).
- FATF Recommendations and industry standards (ABCripto).

4. Governance

- Formal AML/CFT Officer with functional autonomy to conduct analyses, decide on freezing/termination and report to competent authorities.
- Segregation between commercial/operational duties and the compliance function.
- Continuous training program for staff involved in onboarding, monitoring and customer support.
- Whistleblower channel for internal or external reports, with whistleblower protection.

5. Risk-based assessment and monitoring

We perform continuous transaction monitoring based on an internal risk matrix that considers, among other factors: counterparty profile, history, geography, payment instrument, transaction pattern, political exposure and restrictive-list results.

Specific operational parameters (quantitative thresholds, alert rules, granular indicators) are confidential in order to preserve the effectiveness of the control and to prevent reverse engineering by risk actors.

6. Typologies monitored

The policy considers typologies recognized by COAF, the Central Bank of Brazil and the FATF, with focus on the most frequent typologies in the Brazilian P2P market:

- Triangular fraud through misuse of third-party accounts (Pix mule fraud).
- Social engineering and pig butchering.
- Money mule recruitment and post-disaster co-option.
- Structuring/smurfing and coordinated multi-counterparty operations.

7. Reporting to authorities

- Unusual operations or those showing AML/CFT indicators are subject to internal analysis and, when applicable, reported to COAF in accordance with legal criteria.
- Cooperation with competent authorities (Central Bank, Federal Police, Public Prosecution Service, Judiciary) upon formal request.
- Compliance with the tipping-off duty: the customer is not informed about reports submitted to authorities.
- Non-occurrence statement to COAF when required by the applicable regulation.

8. Sanctions screening

We perform systematic screening against official restrictive lists (OFAC, UN, EU and applicable national lists) during onboarding, recertification and continuous monitoring. A positive match that cannot be mitigated leads to refusal or termination.

9. Available measures

- Request additional information and documents (enhanced due diligence — EDD).
- Suspend, refuse or terminate the relationship when risk is non-mitigable.
- Preserve digital chain of custody of related records, with verifiable integrity.

10. Records retention and chain of custody

Documents, transactional records and analysis evidence are retained for the minimum period required by applicable law, observing the purpose of regulatory proof and legal defense. Digital chain of custody is maintained with integrity controls.

11. Training, review and audit

- Continuous technical training for staff involved in compliance and customer support.
- Mandatory annual review of this policy, or upon relevant regulatory change.
- Periodic internal audit; external independent audit may be commissioned when justified.

12. Institutional alignment

This Policy must be read together with Nexus Capital's KYC Policy, Privacy Policy (LGPD) and Terms of Service. The rules of the P2P platforms used and applicable legal duties prevail in case of regulatory conflict.

13. Effective date and final provisions

This Policy is effective on its publication date and remains valid until a new version is issued. Compliance contact: meajuda@nexuscapitalp2p.com.br.

Notice

This document describes the public posture of Nexus Capital regarding AML/CFT. Detailed operational procedures, quantitative parameters, specific alert indicators, internal operational deadlines and technical tooling are confidential information and are not disclosed.