AML & Compliance Policy

Stablerail, Inc. | Version 1.1 | Updated October 30, 2026

This policy sets the required standards for preventing money laundering, terrorist financing, sanctions evasion, fraud and other financial crime in connection with Stablerail's corporate treasury software. It applies to directors, employees, contractors and customers within their respective roles. It is not a representation that Stablerail is a bank, licensed money transmitter or regulated custodian.

1. Scope and service boundaries

Stablerail, Inc. is a Delaware corporation providing corporate treasury software and access interfaces to third-party services. Stablerail does not itself open or provide bank accounts, issue cards, accept deposits or provide bank deposit insurance. Fiat accounts, account details, collections, payouts, conversions and card services, where available, are supplied by the applicable third-party providers under their own agreements, eligibility rules and regulatory responsibilities. A named account or account identifier is not a bank account issued by Stablerail.

The platform supports non-custodial digital-asset workflows. Stablerail does not take custody of customer assets or assume the role of the customer's bank. Restricting platform access is not the same as freezing assets held by a bank or in a self-custodial wallet. Stablerail does not promise to reverse a blockchain transfer or recover assets outside its control.

Regulatory obligations depend on the actual activity, location and contractual role, not on a software label. Before introducing a new jurisdiction, payment flow, custody arrangement or service, management must assess the applicable licensing, AML, sanctions and reporting requirements. A regulated activity must not be launched without the required authorization or a lawful arrangement with an authorized provider.

2. Allocation of responsibilities

Each banking, payment, card or digital-asset partner is responsible for the AML program, customer acceptance, transaction execution, account restrictions and regulatory reporting required for its own services. Partner approval does not automatically approve access to Stablerail, and Stablerail approval does not approve a partner account. Partners may independently request information, reject an application, delay or refuse a payment, restrict an account or end their services.

Stablerail is responsible for obligations applicable to its own activities, platform access decisions, internal escalation and lawful cooperation with partners and authorities. Outsourcing verification or screening does not excuse Stablerail from its own mandatory duties. No partner arrangement transfers liability imposed by law, and Stablerail must not knowingly facilitate prohibited activity.

Customers remain responsible for the legality of their business, ownership and source of funds, their counterparties, authorized users, transaction instructions and any AML obligations applicable to their own business. Stablerail's screening tools and evidence packs support, but do not replace, the customer's independent compliance program or legal advice.

3. Governance and accountability

Management must formally approve this policy, appoint a competent compliance owner in writing and give that person access to relevant information and authority to restrict onboarding or platform access. Commercial staff must not override a compliance rejection or unresolved sanctions concern. High-risk acceptance and any lawful exception require documented compliance review and management approval.

The compliance owner must maintain a risk assessment, escalation register, decision records and a register of relevant providers and responsibilities. Staff must promptly report concerns through compliance@stablerail.com or the designated internal channel. Suspected misconduct must not be concealed, and good-faith reporting must not result in retaliation.

This is a written policy standard, not an attestation of completed controls, a named officer appointment, a regulatory license or a board approval. Formal adoption, operational procedures, assigned responsibilities and evidence of implementation must be recorded separately before this document is presented as proof of an implemented AML program.

4. Risk-based customer acceptance

Business customers must be assessed before access to relevant transactional services and whenever material information changes. The assessment must consider incorporation and operating locations, ownership and control, products, customer base, counterparties, expected amounts and frequency, payment corridors, asset types, delivery channels and adverse information.

Anonymous or fictitious customers, concealed beneficial ownership and unverifiable business purposes are unacceptable. No access to partner banking or payment services may be enabled while required verification or partner acceptance remains incomplete. Access to a demonstration or read-only tool is not transactional approval.

Nationality alone is not a sanctions determination. Eligibility must reflect applicable sanctions, residence, location, ownership, activity and partner restrictions. Stablerail may apply a stricter risk appetite than the minimum required by law and decline a relationship that cannot be assessed or supported safely.

5. Business verification and beneficial ownership

Due diligence must establish the customer's legal name, registration number, legal form, registered and operating addresses, directors, authorized representatives, ownership chain and natural persons who ultimately own or control it. Supporting information may include registry extracts, constitutional documents, ownership charts, identity documents, address evidence and proof of authority.

Beneficial owners must be identified under the applicable legal and partner thresholds, including control by other means. A percentage threshold must not be used to ignore an individual exercising effective control. Where no natural-person owner is identified after reasonable measures, the applicable senior-management identification process and the reasons for using it must be documented.

Business activity, website, intended account use, expected flows, counterparties and source of funds must be consistent with the customer's profile. Unexplained discrepancies, forged documents, nominee structures or unwillingness to disclose ownership require escalation. Verification may be performed by a partner or specialist provider, but reliance must have a lawful basis, defined scope and sufficient access to supporting evidence.

6. Sanctions, PEPs and adverse information

Relevant customers, beneficial owners, controllers, representatives and transaction counterparties must be checked against applicable sanctions and restrictions. These include US sanctions administered by OFAC and other regimes where they apply to the activity or are required by a partner. Ownership and control restrictions must be assessed, including OFAC's aggregate 50 percent ownership rule. Other regimes may use different control tests.

Potential matches must be escalated and resolved with supporting evidence before the affected service is enabled or continued. A true prohibition must not be bypassed by using another partner, wallet, asset, entity or corridor. False-positive decisions must be documented. Required re-screening must address material customer changes, relevant sanctions changes and transaction risk.

Politically exposed persons, their relevant family members and close associates, and credible adverse financial-crime information require risk-based enhanced review. PEP status is not itself a criminal finding. Acceptance requires the appropriate approvals and source-of-funds or source-of-wealth evidence. Screening data can be incomplete or inaccurate and must not be treated as a guarantee of legality.

7. Enhanced due diligence

Enhanced due diligence is required where the risk assessment identifies heightened risk, including opaque ownership, high-risk locations or activities, unusual volumes, adverse information, material third-party flows or uncertain source of funds. It must establish the economic purpose, ownership and control, relevant source of funds and, where appropriate, source of wealth.

Additional evidence may include contracts, invoices, financial statements, tax records, bank statements, licenses, wallet-control evidence and explanations of the underlying commercial relationship. High-risk acceptance requires written approval and a documented monitoring and refresh plan. If the risk cannot be resolved, Stablerail must decline or restrict the relevant service rather than rely on an unsupported explanation.

8. Prohibited use and third-party funds

The platform must not be used for criminal proceeds, terrorist financing, sanctions evasion, fraud, stolen assets, unlawful gambling, unlawful financial services, deliberate concealment of ownership or transaction purpose, or circumvention of checks, reporting requirements or partner restrictions.

The default permitted use is the customer's own corporate treasury. Collecting, holding or moving money for unrelated third parties, operating customer-money accounts, undisclosed payment aggregation and payment-on-behalf arrangements are not permitted unless explicitly approved in writing by Stablerail and the relevant provider, supported by the required licenses or lawful exemptions and fully disclosed due diligence.

Splitting payments to evade review, using false invoices, disguising a counterparty or using a replacement route after a compliance refusal is prohibited. Deliberate use of mixers, obfuscation services or privacy techniques to conceal illicit funds or defeat screening is prohibited. Elevated-risk exposure without demonstrated illicit intent still requires review and may be declined.

9. Digital-asset screening and transaction review

Relevant wallet addresses and proposed digital-asset activity must be assessed using available on-chain risk intelligence and the applicable controls for the service. Review must consider sanctions exposure, stolen assets, ransomware, darknet activity, scams, suspicious obfuscation, direct and indirect exposure and consistency with the customer's business.

Risk scores are indicators, not legal clearance. Material alerts require documented review and must not be dismissed solely because a score is below a commercial threshold. If required screening is unavailable, relevant access or workflows must remain restricted until screening is completed or an alternative lawful control is documented and approved. No exception may authorize activity prohibited by law.

Monitoring must be proportionate to Stablerail's role and the information it can lawfully access. Unusual value, frequency, rapid movement, circular flows, unexplained changes of counterparties or corridors and transactions inconsistent with the business profile require escalation. Partner monitoring does not replace review of concerns actually known to Stablerail.

10. Escalation, restrictions and reporting

Staff must escalate suspected financial crime or sanctions exposure promptly to the compliance owner, preserve relevant records and avoid unauthorized communications that could compromise a review. The compliance owner must record the facts, actions, relevant partner notifications and the rationale for the decision.

Stablerail may restrict platform access, disable affected workflows, decline new instructions and request additional evidence within its contractual and technical powers. A partner may separately hold, block, return or refuse funds under its own authority. Stablerail cannot release a partner's hold, guarantee a review deadline or promise a refund, recovery or reversal of an executed transfer.

Where a report is legally required from Stablerail, the responsible person must make it to the competent authority within the applicable deadline. Reports belonging to a partner's regulated activity are that partner's responsibility. A referral to a partner does not discharge a separate reporting duty imposed on Stablerail. Reporting obligations must be determined for the actual activity, not assumed from this policy.

Confidential reports and investigations must not be disclosed where prohibited by law. Customer communications may be limited to lawful requests for information or service-status notices. Staff must not promise that a report has or has not been filed.

11. Partner diligence and cooperation

Before enabling a partner service, Stablerail must assess the provider's identity, relevant authorizations, supported jurisdictions and activities, contractual allocation of responsibilities, onboarding requirements, restrictions and escalation arrangements. The assessment and material changes must be documented. A partner's brand, bank relationship or marketing statement is not a substitute for verification.

Contracts and operational arrangements must define who performs customer verification, maintains evidence, screens and monitors relevant transactions, handles regulatory reports and responds to requests. Stablerail must not represent that it operates a partner's AML program or guarantees partner acceptance.

Stablerail may lawfully share necessary customer, ownership and transaction information with relevant providers and authorities under the applicable contractual and privacy framework. Customers must cooperate with legitimate requests. A refusal, incomplete response or misleading information may result in restricted access or termination.

12. Customer undertakings and contractual protection

Customers must provide accurate, complete and current information, promptly disclose material changes and supply evidence requested for verification or review. They must ensure that users are authorized, funds are lawfully obtained, payments have a genuine lawful purpose and activities comply with applicable law and provider terms.

A Stablerail subscription, risk report, screening result or evidence pack is not regulatory approval, a legal opinion, a guarantee of transaction acceptance or confirmation that an account or asset is insured. Customers must not describe Stablerail as their bank or use Stablerail's name to imply a license or authorization it does not hold.

Subscription fees purchase self-custodial treasury software and platform tools, not guaranteed bank accounts. Partner banking and payment services require separate KYB/KYC review, provider terms and provider approval. A partner's delay, rejection, restriction or withdrawal does not, by itself, entitle a customer to a subscription refund or automatically cancel the subscription. Billing continues until cancellation takes effect under the applicable terms. Customers may continue using eligible software features subject to law, sanctions, security, provider requirements and the service terms, or cancel under their subscription terms. Mandatory legal rights, express written refund or termination rights and remedies for Stablerail's own breach remain unaffected. This policy does not amend an already executed agreement.

Any exclusions of liability, allocation of losses, indemnities, fees and termination rights are governed by the applicable executed agreement and enforceable service terms, subject to mandatory law. This policy does not create an unlimited indemnity, change an agreed liability cap or excuse Stablerail's own unlawful conduct. Stablerail does not assume a partner's duties merely by displaying or facilitating access to that partner's service.

13. Records, privacy and information security

Stablerail must maintain adequate records of customer review, verification evidence it holds or may lawfully access, risk assessments, alerts, restrictions, approvals, escalations and relevant communications. Audit-trail and Proof-of-Control records are retained for a minimum of seven years as described in the Privacy Policy. Other AML records follow the applicable legal and contractual retention period and documented retention schedule, with longer preservation where required by a lawful hold.

Compliance information must be protected by appropriate access controls and shared only where necessary and lawful. Data collection, international transfers and retention must respect applicable privacy requirements. Staff must never request a customer's seed phrase or private key as an AML document. Records must be sufficient to reconstruct the basis for a material decision without exposing sensitive investigations publicly.

14. Training, review and remediation

Relevant staff and contractors must receive training before undertaking compliance-sensitive responsibilities and at least annually thereafter. Training must cover customer risk, sanctions, digital-asset red flags, escalation, confidentiality, data handling and partner-role boundaries. Completion must be recorded.

Management must arrange a suitably independent review of the policy and its implementation at least annually and after material changes or incidents. The reviewer must not review only their own work. Findings, corrective actions, accountable owners and completion evidence must be recorded. No employee may certify that controls operate effectively without supporting evidence.

15. Legal precedence and policy changes

Mandatory law takes precedence over this policy. Applicable executed customer agreements and provider terms govern the respective services, but cannot authorize prohibited activity or waive mandatory duties. This policy must be read with Stablerail's Terms of Use and Privacy Policy and does not grant a right to service or a guaranteed outcome.

Management must review this policy at least annually and when services, partners, risk exposure or legal requirements materially change. Changes must be versioned and communicated to relevant personnel. Local procedures or contractual controls may be stricter than this public policy, but may not weaken a mandatory requirement.

16. Contact

Compliance enquiries and reports of suspected misuse should be sent to compliance@stablerail.com. Stablerail, Inc., 131 Continental Dr, Newark, DE 19713, USA. Do not send private keys, seed phrases or unnecessary sensitive identity documents through ordinary email.