Safeguarding of Client Assets Policy

NOVARA, S.A. DE C.V.

El Salvador

August 2025

Table Of Contents

Introduction

The purpose of this policy is to ensure that NOVARA, S.A. DE C.V (the Company) takes all reasonable precautions to protect customer assets against any eventualities and threats. The Company will also have to ensure that the customer assets are properly accounted for.

The Board of Directors or the Unique Administrator of the Company will be responsible for the safeguarding of customer assets and the adherence to this policy. The CFO will also ensure that daily reconciliations take place, and that Client assets and monies are held separately from the Company's own assets. The Compliance Officer is additionally responsible for overseeing adherence to applicable safeguarding obligations under the Comisión Nacional de Activos Digitales (CNAD), the Superintendencia del Sistema Financiero (SSF), and international AML/CFT standards.

This Policy applies across all departmental operations and to all departmental staff, consultants and contractors. It also extends to outsourced service providers, including Custodians, Liquidity Providers, and Payment Service Providers (PSPs/EMIs), who must comply with equivalent safeguarding and segregation requirements.

General Principles

The objectives of the Company in the context of safeguarding and segregation of client assets are the following:

- protect the clients' assets against any eventualities and threats;
- ensure that the clients' assets are sufficiently liquid so that they can be returned upon request.
- ensure that all safeguarding and segregation practices comply with applicable regulatory requirements of CNAD, SSF, and relevant AML/CFT obligations.

The Company approach to client money and assets is driven by the following principles:

- overall responsibility for client assets has been nominated to the Senior Management;
- the systems and controls in place are appropriate and proportionate to the nature and size of the business;
- client assets are held separately and appropriately segregated from the Company's own assets;
- custodial assets are clearly designated & easily identifiable;
- custodial assets are protected from third party creditors;
- daily reconciliation is performed over client assets and the Company's own assets;
- Records are stored safely within a naming and schema allowing for clear audit trail.
- reconciliations and safeguarding procedures are subject to oversight by the Compliance Officer, Internal Audit, and, where required, external regulators;
- third-party custodians, PSPs/EMIs, and liquidity providers must provide assurance (e.g., SOC/ISAE audit reports) that safeguarding controls are effective.

Safeguarding & Segregation of Assets

The Company will ensure that the custodial assets and monies are held separately from the Company 'own assets and are reconciled daily.

The Company will ensure that fiat currency is held with a regulated credit institution. Therefore, Client fiat currency will be held separately from the rest of the Company funds. For digital assets, Client assets will be held in a separate address, stored independently in wallets under the custody of the Company and its trusted counterparties. Custodial arrangements must include multi-signature or MPC (multi-party computation) technology to minimise single point of failure risks.

The Company maintains digital wallets to store the clients' digital assets. The private keys are encrypted by an encryption algorithm before storing in the database, and the encryption key is isolated with access limited to one member of staff and one back-up. Access to keys and signing procedures must always require dual control, with segregation of duties between operations and compliance.

The Company understands that if a third party is used to store or safeguard customer assets, the Company shall ensure that the systems and controls used by the third-party provider(s) are effective. This includes contractual obligations for the provider to segregate Novara's client assets from its own, provide audit reports, and notify any incidents immediately.

The Company acknowledges and understands that the Client assets do not represent property of the Company and must therefore be protected from the Company's third-party creditors.

The Company recognises the need to safeguard and segregate all client assets from its own and in doing so, has considered the operational implications for each relevant department. These safeguarding practices are subject to regulatory review by CNAD and SSF, and internal/external audits.

Third-Party Custodians

In case the Company decides to use third party custodians to safeguard client assets, it will still be the Company's responsibility to ensure that they are doing so properly. Therefore, the following procedures are performed over all third-party custodians:

- review of history, background and other due diligence procedures;
- undertake a number of meetings with the third-party custodian;
- ensure adequate and appropriate controls in place to safeguard assets;
- ensure adequate and appropriate levels of insurance is in place; and
- review draft contract terms to ensure adequate and appropriate levels of protection, obligations and responsibilities are clearly defined and documented.
- verify that the custodian segregates Novara's client assets from its own assets and from assets of other clients, ensuring clear identification at all times;
- obtain and periodically review independent assurance reports (e.g., SOC 1/SOC 2, ISAE 3402) on the custodian's controls;
- establish contractual obligations for incident reporting, regulatory cooperation, and data protection compliance (including Travel Rule and AML/CFT requirements).

Any additional procedures will be determined during the outsourcing process. Custodian relationships must be approved by Senior Management, monitored by the Compliance Officer, and reported to regulators when required.

Insurance

In addition to the use of third-party custodians, the Company shall consider the need to purchase its own insurance to reduce its overall exposure to crypto assets to acceptable and established levels. The amount and level of insurance cover required shall be appropriate, proportionate and relevant, and reviewed on an on-going basis depending on levels of client assets held by the Company and the availability of cost-effective insurance cover.

Systems and Controls

The Company has created appropriate systems and controls to manage client assets that are proportionate to the size of the business, the assets in custody and the risks involved in that business.

Ensuring security of clients and employees is of the utmost importance to the Company, as well as the prevention of any fraud or cybercrime. The Company therefore aspires to the highest security level in order to minimize possible security breaches.

Systems and controls shall include: segregation of client funds, multi-factor authentication (MFA), role-based access controls, encryption of sensitive data, continuous monitoring, and independent internal audit reviews.

Special emphasis is placed on outsourced or cloud-based services (Custodians, PSPs/EMIs, Liquidity Providers, and KYT vendors), which must comply with equivalent or higher security standards, and are subject to periodic due diligence and contractual obligations.

The Compliance Officer and Information Security Officer (ISO) are jointly responsible for monitoring the effectiveness of these systems and controls, and for reporting deficiencies to Senior Management and, where required, CNAD or SSF.

IT and Software

The following controls shall be considered to detect fraud and cybercrime are as follows:

- employees are required to secure the Company's accounts with passwords;
- clients will generate a unique password for their account and are strongly reminded not to share their passwords within anyone else;
- establish solutions that prescribe for or combine both verification and authentication technologies to ensure secure online testing;
- maintain user protection by utilizing multi-signature technology and user security codes;
- patterns analysis on traffic to servers;
- IP checking;
- looking for brute force attacks on passwords;
- multilevel security checks on clients that requests access to their accounts;

- undertake resiliency testing and penetration tests.
- continuous monitoring of servers, APIs, and third-party integrations (Custodians, PSPs/EMIs, KYT providers) through a Security Information and Event Management (SIEM) system;
- regular patch management and vulnerability scans with documented remediation timelines (e.g., critical CVEs patched within 24 hours).

Systems of control related to IT and software shall always be kept up to date and meets latest industry protocols and standards. Compliance with ISO 27001, IEC 22301, and NIST Cybersecurity Framework is targeted, and external audits or certifications will be pursued where required by regulators or institutional partners.

Digital Wallet Controls

The following controls shall be considered to secure client digital wallets and assets held on these wallets:

- each client will be assigned a unique wallet address for transferring his digital assets into the firm ecosystem;
- the Company will control private keys for the clients, and these private keys are encrypted before stored in the database;
- the private keys for client's wallets are not transmitted over the network;
- all transaction signings are done on the server and only the result will be transmitted over the Internet to the blockchain network;
- the encryption key is stored in a secure network that has no direct internet connection;
- only one authorised person and one back-up can have access to the platform servers and the encryption key.
- custodial arrangements must leverage multi-signature or MPC (multi-party computation) technology, ensuring that no single individual can unilaterally move client assets;
- private keys and signing processes must be subject to dual-control, segregation of duties, and monitoring by the Information Security Officer and Compliance Officer;
- all wallet operations (deposits, withdrawals, transfers) must be logged in immutable audit trails, reviewed daily, and subject to exception reporting;
- cold storage solutions must be used for long-term asset holdings, with strict access controls and geographic redundancy;
- hot wallet balances must be limited to operational needs, with automatic sweeps to cold or warm storage.

Systems and Controls Stress testing

The Company shall perform periodic stress and scenario testing to identify inherent operational weaknesses and process inefficiencies. Stress testing must include scenarios of custodian failure, payment processor disruption, liquidity provider unavailability, and cyberattacks impacting client asset safeguarding.

On a quarterly basis, meetings must be held with department heads from the functions listed below to review and update relevant stress scenarios and consider ongoing control effectiveness.

Controls across following functions are reviewed in scenario testing:

- finance Function (i.e. Accounting);

- operations Function (i.e. Reconciliations model);
- ICT Function (i.e. Software platform, reporting functionalities).
- compliance Function (i.e. AML/CFT transaction monitoring, Travel Rule data exchange, suspicious activity escalation).

The (outsourced) Internal audit function shall periodically test the operating effectiveness of the internal controls. Results of stress testing and audit reviews must be documented, reported to Senior Management, and made available to CNAD or SSF upon request.

Reconciliations

The Company shall perform a number of reconciliations over the digital assets held by the Company. The following 3-way reconciliation shall at least be considered and created by the designated team:

- software platform;
- ledger balance; and
- accounting package
- custodian wallet balances and transaction reports (for assets held with Fireblocks, BitGo, or other third-party custodians);
- bank/PSP/EMI statements for fiat assets.

An exception-based report is also reviewed and analysed on a daily basis and forms a key part of the daily reconciliation. All reconciliation discrepancies must be escalated immediately to the CFO and Compliance Officer, investigated within 24 hours, and documented with corrective actions.

Monthly reconciliation reports shall be presented to Senior Management and made available to CNAD and SSF upon request.

Version Control Table

Approval date	Changes description	Senior Manager's signature
27.08.2025	First issue	