NURCOIN®

Security Framework

Official Security & Governance Document

Version 1.0 - December 2025

https://nurcoin.ai | https://nurcoin.co

NURCOIN® • Security Framework

Legal-Grade Security • AI-Assisted Risk Control • Compliance-by-Design

This document outlines the security principles, architectural controls, and governance posture applied within the NURCOIN® ecosystem.

Official Security & Governance Document

Version 1.0 – December 2025

https://nurcoin.ai

https://nurcoin.co


NUR
NURCOIN
BANK
AML
KYC
NURCOIN®
SECURITY
FRAMEWORK
UTC
24/7

Brand Authenticity & Legal Identification

NURCOIN® is the official registered brand of the NURCOIN ecosystem.

Trademark status:
European Union Trademark (EUTM) Application
Application No. 019088455

Official platforms:
https://nurcoin.ai — informational, documentation, and governance materials
https://nurcoin.co — financial operations and transactional services
Legal Entity Identification (LEI)

The operating entity associated with NURCOIN® holds an active Legal Entity Identifier (LEI), supporting institutional transparency and global financial interoperability.

LEI Code: 98450055CF6DYA5EBF29
LEI Registration Status: ACTIVE
Issued On: 05 March 2025

Registered Legal Name: Papian Karen

Legal Jurisdiction: Greece (GR)

Entity Legal Form: Sole Proprietor

Registration Authority: Independent Authority for Public Revenue (AADE), Greece

The LEI record is published within the GLEIF global database and enables standardized identification for regulatory, banking, and compliance-related interactions

Contextual Note (small text at bottom of slide)

The inclusion of LEI information supports transparency, audit readiness, and institutional-grade governance.

This document is provided for informational purposes and reflects the current operational posture of the NURCOIN® ecosystem.

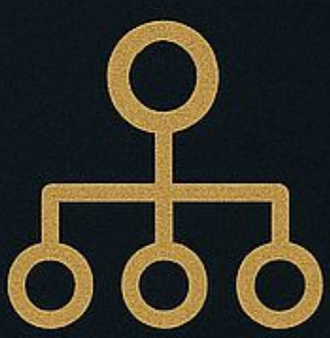
AML COMPLIANCE

ESSENTIAL MEASURES FOR AML COMPLIANCE

CUSTOMER DUE DILIGENCE

TRANSACTION MONITORING

AML POLICY



STAFF TRAINING

PURPOSE & SCOPE

The NURCOIN® Security Framework defines the principles, controls, and operational posture applied to protect the NURCOIN® ecosystem.

The framework covers security considerations across:

- Blockchain infrastructure
- Platform and application services
- Smart contract logic
- Digital assets and transaction flows
- Identity and access processes
- Security-relevant operational workflows

This document is provided for informational purposes only and may evolve depending on development phase, jurisdictional requirements, and regulatory alignment.

CORE SECURITY PRINCIPLES

Security within the NURCOIN® ecosystem is treated as a system-level property, embedded into design, architecture, and operational processes.

The framework is guided by the following core principles:

Defense-in-Depth
Multiple independent security layers are implemented to reduce single points of failure.

Privacy-by-Design
Data protection principles are integrated from the earliest stages of system design.

Traceability
Security-relevant actions are recorded, traceable, and auditable.

Continuous Monitoring
Security posture is maintained through ongoing detection, analysis, and improvement.

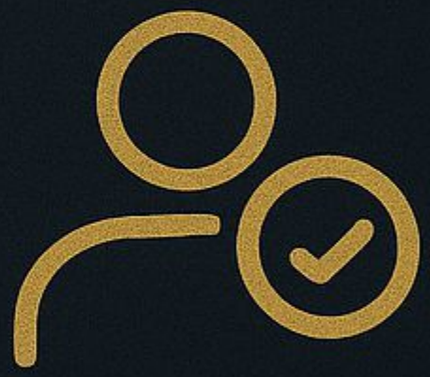
Audit Readiness
Controls are designed to support verification, investigation, and regulatory review.

BENEFITS OF AML COMPLIANCE

REGULATORY COMPLIANCE

REDUCED RISK

PROTECTION FROM FINES



IMPROVED REPUTATION

Security Philosophy

NURCOIN® does not treat security as an add-on or reactive function.

Instead, security is approached as a foundational requirement that informs:

- Architectural decisions
- Development practices
- Operational workflows
- Governance structures

This philosophy aligns with best practices observed in regulated financial, fintech, and digital asset environments, where trust and resilience are critical.

Threat Model Overview

The security framework addresses common risks present in decentralized finance and digital platforms.

Threat categories include:

- Unauthorized access and credential abuse
- Smart contract logic exploitation
- Transaction manipulation and abuse
- Identity misuse and social engineering
- Operational errors and misconfiguration
- Insider misuse or privilege escalation
- Third-party and dependency-related risks

Threat modeling is an iterative process and is updated as the ecosystem, threat landscape, and regulatory environment evolve.


AML
KYC
RISK
REGULATORY PRESSURE
CURRENT LANDSCAPE (2025)
Enforcement Actions

Security Architecture Layers

NURCOIN® applies a layered security architecture to ensure resilience and isolation of risk.

Infrastructure Layer

Hardened hosting environments, network segmentation, availability monitoring, and fault isolation are applied to protect underlying systems.

Application & Platform Layer

Secure coding practices, role-based access controls, session protection, and abuse prevention mechanisms are implemented at the application level.

Smart Contract Layer

Smart contracts are designed with explicit permission models, controlled dependencies, and pre-deployment review considerations.

Each layer operates independently while reinforcing overall system security.

Cryptographic Foundations

NURCOIN® relies on industry-standard cryptographic primitives to secure digital assets and transactions.

These include:

- Secure hashing
- Asymmetric cryptography
- Digital signatures
- Cryptographic randomness

Key handling principles include:

- Private keys are never intentionally exposed
- Least-exposure access boundaries
- Key rotation and revocation capabilities
- Auditability of privileged cryptographic operations


10%
QUANTIFYING REGULATORY COSTS
(2025)
25%
2021

Identity, Access & Authentication

Access to NURCOIN® systems is governed through controlled identity and access mechanisms.

Security measures include:

- Role-based access controls
- Strict separation of privileged access
- Enhanced verification for sensitive actions
- Protection against brute-force and abuse attempts

Where applicable, identity and access controls are aligned with jurisdictional compliance requirements.

AI-Assisted Security Monitoring

Artificial intelligence is used as a supporting security layer within the NURCOIN® ecosystem.

AI-assisted capabilities may include:

- Transaction pattern analysis
- Anomaly detection
- Behavioral risk scoring
- Alert prioritization

AI outputs are subject to human review and governed through defined operational procedures to preserve accountability and control.

This approach aligns with the AI integration principles outlined in the NURCOIN® Whitepaper v3.1.


STRATEGIES
FOR COMPLIANCE
(2025)
ENHANCED MONITORING
PROCESS AUTOMATION
TRAINING PROGRAMS

Data Protection & Privacy

NURCOIN® adopts privacy-by-design principles consistent with GDPR and EDPB guidance.

Core practices include:

- Data minimization
- Purpose limitation
- Controlled access
- Encryption where applicable
- Secure retention and disposal policies

Data protection practices may vary depending on service scope, operational phase, and jurisdiction.

Logging, Monitoring & Auditability

Security-relevant events within the NURCOIN® ecosystem are handled through structured logging and controlled audit access.

Objectives include:

- Time-based traceability of actions
- Event correlation and investigation
- Controlled visibility of sensitive logs
- Support for audit and regulatory review

These measures enhance operational resilience and accountability.

REGULATORY CHALLENGES AHEAD

(2025)

Incident Response & Resilience

NURCOIN® follows a structured incident response lifecycle:

1. Detection and classification of security events
2. Containment and isolation of affected components
3. Impact assessment and analysis
4. Corrective actions, including remediation and credential rotation
5. Post-incident review and improvement

This lifecycle supports rapid response, transparency, and continuous security improvement.

Governance & Responsibility

Security governance within NURCOIN® is supported through defined responsibilities and controlled decision-making.

Key governance elements include:

- Defined roles for security governance and operations
- Separation of duties for sensitive workflows
- Change control procedures for significant updates
- Traceability of configuration and policy changes
- Continuous review and improvement processes

Governance practices are aligned with regulated operational environments.

NAVIGATING THE REGULATORY ENVIRONMENT

Relationship to Other Documents

This Security Framework complements other official NURCOIN® documents, including:

- NURCOIN® Whitepaper v3.1
- Legal & Compliance Disclosures
- Privacy Statements
- Risk Disclosures

Together, these documents provide a comprehensive view of the ecosystem's design, governance, and operational posture.

Contact & Official Channels

For questions regarding the NURCOIN® Security Framework or official documentation, please contact:

NURCOIN® Support & Information Team
Irodotou 19, Nea Alikarnassos
71 601, Heraklion, Crete, Greece

Telegram: NURCOIN® Official
WhatsApp: +30 698 148 3519 | +30 697 264 2530
Email: support@nurcoin.ai | support@nurcoin.co


NURCOIN
NURCOIN
NURCOIN
NURCOIN® Support
Irodotou 19, Nea Alikarnassos
71 601, Heraklion, Crete, Greece
Telegram: NURCOIN® Official
WhatsApp: +30 698 148 3519 | +30 697 264 2530
Email: support@nurcoin.ai | support@nurcoin.co