

Crypto Risk Policy

Surewin B.V.

Table of contents

Crypto Risk Management Policy	4
1. Purpose and Objectives.....	4
2. Scope	5
3. Governance and Responsibilities	5
4. Supported Cryptocurrencies.....	6
5. Customer Identification (KYC).....	6
5.1 Minimum Verification Requirements	6
5.2 Trigger Events for Enhanced Verification.....	7
5.3 Wallet Management.....	7
5.4 Transaction Controls	8
5.5 Sanctions Screening	9
5.6 FATF Travel Rule / VASP Controls	9
5.7 Prohibited Activities	9
6. Financial and Market Risk Controls	10
7. Incident Response	10
Incident Management Steps:	10
8. Reporting & Record-Keeping	10
9. Training and Awareness.....	11
10. Audit and Review.....	12
11. Responsible Gambling	12
12. Third-Party Risk Management.....	13
13. Continuous Improvement.....	13
14. Data Protection.....	13
15. Policy Enforcement	13
16. Amendments	14

Version no.	Issue date	Issued by	Amendment - Whole - Partial
1	21/05/2026	Craig Murugan	New

Crypto Risk Management Policy

1. Purpose and Objectives

This Crypto Risk Management Policy establishes the governance framework, procedures, and control measures to identify, assess, monitor, and mitigate risks associated with cryptocurrency use within **Surewin B.V.** online gaming operations.

The purpose of this Policy is to:

- Prevent money laundering, terrorist financing, fraud, and sanctions violations;
- Ensure compliance with Curaçao gaming regulations and applicable AML legislation;
- Protect customers and the integrity of the gaming platform;
- Define operational controls for crypto deposits and withdrawals.

This Policy is implemented in accordance with:

The Landsverordening Identificatie bij Dienstverlening (LID) concerning customer identification and verification requirements; The Landsverordening Melding Ongebruikelijke Transacties (LMOT) concerning the reporting of unusual transactions; The Curaçao Gaming Authority (CGA) AML/CFT Regulations (January 2025) and related supervisory guidance; Applicable guidance issued by the Financial Intelligence Unit Curaçao (FIU Curaçao); Relevant Financial Action Task Force (FATF) Recommendations relating to virtual assets, virtual asset service providers (VASPs), and risk-based AML/CFT controls; and Any other applicable laws, regulations, directives, or licensing obligations governing cryptocurrency activities.

This policy ensures:

- Compliance with Curaçao eGaming licensing obligations and AML/CTF standards. Protection of player funds and company assets.
- Prevention of misuse of the platform for money laundering, terrorism financing, or sanctions evasion.
- Operational resilience and integrity of crypto systems.
- Responsible management of financial and technological exposures unique to virtual assets.

2. Scope

This policy applies to: All business units of **Surewin B.V.**, including payments, finance, compliance, product, IT security, VIP, and customer service. All cryptocurrency activities, including deposits, withdrawals, conversions, wallet management, and affiliate payments. All employees, contractors, and third-party service providers engaged in crypto-related processes. All customers accessing the casino, regardless of location.

This policy complements and should be read in conjunction with: AML/CFT Policy and Responsible Gambling Policy

3. Governance and Responsibilities

Role	Responsibilities
Board of Directors	Approve and oversee this policy, set risk appetite, review periodic risk reports.
Chief Compliance Officer (CCO)	Maintain the risk framework, oversee implementation, monitor compliance, liaise with regulators, and report incidents.
Risk & Compliance Committee	Conduct quarterly reviews, maintain risk register, and evaluate control effectiveness.
Head of Finance / Payments	Ensure reconciliation of crypto funds, maintain wallet segregation, manage liquidity and conversion risk.
Head of IT/Security	Maintain secure custody solutions, implement access control, and oversee technical risk mitigation.
All Staff	Understand and adhere to crypto-related controls, report suspicious or anomalous activity immediately.

4. Supported Cryptocurrencies

The Casino may accept approved cryptocurrencies including, but not limited to:

- Bitcoin
- Ethereum
- XRP
- USDT
- USDC
- SOL

The Casino reserves the right to:

- Reject transactions associated with sanctioned or suspicious wallet addresses.
- Multiple accounts are linked;
- Blockchain analytics indicate elevated risk;
- The customer is located in a high-risk jurisdiction.
- Add or remove supported assets at any time;
- Suspend transactions involving high-risk or privacy-enhanced coins;

5. Customer Identification (KYC)

The Casino shall implement a risk-based Know Your Customer (KYC) program.

5.1 Minimum Verification Requirements

Customers may be required to provide:

- Full legal name;
- Date of birth;
- Residential address;
- Government-issued identification;
- Proof of address;

- Source of funds documentation where applicable.

CDD required for:

- Deposits or withdrawals > €2,000 equivalent
 - High-risk wallets
 - FATF high-risk jurisdictions
- Source of Funds verification for large or repeated transactions.

5.2 Trigger Events for Enhanced Verification

Enhanced Due Diligence (EDD) may be required when:

- Large deposits or withdrawals occur;
- Unusual betting activity is detected;
- Multiple accounts are linked;
- Blockchain analytics indicate elevated risk;
- The customer is located in a high-risk jurisdiction.
- Politically Exposed Persons (PEPs)
- Suspicious activity indicators
- Structuring behavior

Additional verification may include:

- Source of funds
- Source of wealth
- Blockchain transaction history
- Video verification

5.3 Wallet Management

- Operate segregated hot, warm, and cold wallets.
- Maintain multi-signature access (minimum 2 of 3 signatories).
- Dual approval required for withdrawals exceeding thresholds.
- Daily reconciliation and immutable audit logging.
- Hardware-based authentication for wallet access.

5.4 Transaction Controls

- Screen all inbound/outbound transactions using blockchain analytics tools.
- Block or reject funds linked to mixers, darknet services, or blacklisted wallets.
- Enforce velocity limits and confirmation depth before crediting.

Deposits

- Deposits must originate from wallets controlled by the customer;
- Third-party deposits may be rejected;
- Minimum and maximum transaction limits may apply.

Withdrawals

- Withdrawals may require identity verification;
- Withdrawals may only be sent to wallets verified as belonging to the customer;
- The Casino may delay withdrawals pending compliance review.

Important Crypto Risks:

- Irreversible transactions
- Wallet compromise
- Fraud
- Money laundering
- Social engineering
- Phishing
- Chain-hopping
- Mixer/tumbler exposure

5.5 Sanctions Screening

- Screen all customers and wallets against UN, EU/UK, and OFAC sanctions lists.
- Automatically freeze transactions pending review if a match is detected.

Surewin B.V shall not knowingly provide services to:

- Individuals or entities subject to international sanctions;
- Customers from prohibited jurisdictions;
- Persons identified on applicable sanctions lists.

Surewin B.V reserves the right to block accounts and transactions that present sanctions risk.

5.6 FATF Travel Rule / VASP Controls

- The Company shall only transact with VASPs that support secure exchange of originator and beneficiary information in compliance with FATF Recommendation 16 (Travel Rule).
- Transactions missing Travel Rule metadata must be paused and escalated to Compliance.

5.7 Prohibited Activities

The following activities are prohibited:

- Use of stolen or unauthorized funds;
- Use of mixers or tumblers intended to conceal transaction origins;
- Fraudulent gameplay or bonus abuse;
- Transactions involving sanctioned persons or jurisdictions;
- Money laundering or terrorist financing.

6. Financial and Market Risk Controls

- Convert excess crypto balances to stablecoin or fiat to control volatility.
- Maintain liquidity buffer of at least 150% of average daily withdrawals.
- Daily price revaluation and stop-loss triggers.
- Monitor exchange counterparties for solvency and operational risk.

7. Incident Response

An incident includes unauthorized wallet access, sanctions-hit wallets, AML breaches, cybersecurity compromises, or suspicious player behavior.

Incident Management Steps:

1. Detect
2. Contain (freeze accounts)
3. Investigate (forensics)
4. Report **Unusual Transaction Reports (UTRs)** via **goAML** to FIU Curaçao **within 24 hours** when required
5. Recover
6. Review and strengthen controls

8. Reporting & Record-Keeping

- Reported to relevant regulatory or enforcement authorities;
- Result in account suspension or closure;
- Subject to freezing or withholding of funds pending investigation.

- Maintain audit logs, Customer identification, Wallet addresses, Compliance investigations, unusual transaction reports and transaction history for **minimum 5 years**.
- Monthly risk reporting to the Board includes flagged wallets, unusual transaction reports submissions, and crypto exposure.

9. Training and Awareness

Mandatory annual training conducted ensuring all new employees understand:

- The casino's regulatory obligations
- Crypto-related operational risks
- AML/KYC requirements
- Information security responsibilities
- Responsible gambling obligations

Crypto-Specific Red Flags

Employees are trained to identify:

- Multiple accounts using same wallet
- Sudden high-value deposits
- Minimal gameplay followed by withdrawal
- Use of mixing services
- High-risk jurisdictions
- Structuring deposits
- Frequent wallet changes
- Use of privacy coins
- Sanctions exposure indicators

Fraud Prevention Training

Account Fraud

- Identity theft
- Synthetic identities
- Multi-accounting
- Bonus abuse

Payment Fraud

- Stolen crypto

- Compromised wallets
- Fraudulent withdrawals

Social Engineering

Examples:

- Fake executive requests
- Fake support tickets
- Credential harvesting
- Impersonation attacks

Required Controls

Employees must:

- Verify customer identity
- Follow escalation procedures
- Never bypass controls
- Report suspicious conduct immediately

10. Audit and Review

- Internal audit annually.
- Independent external review recommended.
- Remediation actions are completed within 60 days.

11. Responsible Gambling

Crypto and fiat players are subject to the same player protection rules.

The Casino supports responsible gambling measures including:

- Deposit limits;
- Self-exclusion tools;
- Account cooling-off periods;
- Monitoring for harmful gambling behaviour.

12. Third-Party Risk Management

- Conduct due diligence on wallet providers, processors, and exchanges.
- Require AML/CTF controls and contractual right to audit.

13. Continuous Improvement

- Track updates in regulatory guidance and developments.
- Adjust monitoring and controls to evolving crypto typologies.

14. Data Protection

Customer information shall be:

- Stored securely;
- Protected against unauthorized access;
- Processed in accordance with applicable data protection laws.

15. Policy Enforcement

Violation of this Policy may result in:

- Account suspension;
- Transaction rejection;
- Confiscation of illicit funds where legally permitted;
- Reporting to regulatory authorities.

16. Amendments

Surewin B.V. reserves the right to amend this Policy at any time in order to comply with:

- Regulatory requirements;
- Licensing conditions;
- Operational or security requirements.

Updated versions shall become effective upon publication on the Casino website.