

SECURITY POLICY

This Security Policy is addressed directly to you, the player, to explain your responsibilities and what measures we take to protect you and the integrity of our platform. While we implement stringent security measures based on Curaçao law (LOK) and best practices from regulated jurisdictions, we cannot assume responsibility for losses or breaches caused by your own errors or negligence.

1. Account and Password Security

- You are required to use strong, unique passwords on our platform; they must be at least 8 characters and include uppercase/lowercase letters, numbers. Passwords must not match your username.
- Accounts are locked after multiple failed login attempts, and sessions auto-terminate after periods of inactivity.

Your responsibility: Do not share your credentials and use secure devices and networks to access your account.

2. Data Protection and Privacy

- All personal and financial data are stored and transmitted securely, often in encrypted formats.
- We comply with applicable privacy and data-protection laws.

Your responsibility: Keep your email and profile up to date. Notify us immediately of any unauthorized access or suspicious activity.

3. Platform Security and Infrastructure

- We maintain system logs, conduct regular vulnerability assessments firewalls both online and internal system, with 24/7 monitoring Network Operations, protected by fortinet and cloudflare
- We aim for “**security by design**”, ensuring that our infrastructure and applications adhere to best practice technical standards protected by fortinet and cloudflare.

Your responsibility: Do not attempt to circumvent system limitations or exploit vulnerabilities; it may lead to suspension or termination.

4. Incident Reporting and Response

- We follow a formal incident escalation process. From a breach affecting player confidentiality or any service outage exceeding 12 hours, we will report the incident to Curaçao authorities in accordance with regulatory obligations.

Your responsibility: Promptly report any suspected security incident, account breach, or suspicious transaction.

5. Secure Crypto Operations

- All crypto deposits and withdrawals are monitored using blockchain analytics and transaction monitoring to detect suspicious behavior or compliance violations.
- Wallet screening prevents use of addresses associated with sanctioned entities, mixers, or darknet activity. Risk and Fraud team manage and inspect all transactions and all transactions are blockchain protected.

Your responsibility: Only transact using wallets you control. Do not attempt to use wallets flagged or linked to high-risk services.

6. Ongoing Monitoring and Audits

- Our security protocols are reviewed periodically, and independent audit firms examine our system, controls, and compliance with AML/CFT, privacy, and security obligations.
- Our System goes through penetration tests twice per year, and we have certified cyber security personnel inhouse to maintain securely the system.

Your responsibility: Cooperate with verification requests related to audits or compliance checks as needed.

7. Disclaimer & Limitation of Liability

- Internal systems and hosting is maintained via 2FA protections for teams and secure SSL VPN.
- **However, we are not liable for losses arising from:**
 - Compromised private keys or shared credentials
 - Phishing, social engineering, or fraudulent schemes
 - Using insecure devices or networks
 - Your actions or misuse of the platform

Your responsibility: Implement your own personal wallet and device security practices diligently. We provide services, not individual security education.