

INFORMATION SECURITY POLICY

Version 1.0

Effective Date: May 2026

1. Purpose

This Information Security Policy ("Policy") establishes the principles and controls adopted by K.I.K. Corporation B.V. to protect the confidentiality, integrity, and availability of information, systems, player data, and operational processes.

The Policy is implemented in accordance with applicable Curaçao regulatory requirements, including obligations arising under the Curaçao Gaming Authority ("CGA") licensing and AML/CFT framework.

Holzman Limited acts as an independent representative and payment services support provider to K.I.K. Corporation B.V.

2. Scope

This Policy applies to:

- All systems, platforms, applications, and operational processes used by the Company;
- All employees, contractors, service providers, and authorized third parties with access to Company systems or information;
- All customer and transaction data processed in connection with the Company's operations.

3. Information Security Objectives

The Company aims to:

- Protect player and business information from unauthorized access, disclosure, misuse, alteration, or destruction;
- Maintain secure operational and payment-processing environments;
- Prevent fraud, cyber threats, and unauthorized activities;
- Ensure compliance with applicable legal, regulatory, AML/CFT, and responsible gaming obligations;
- Maintain operational continuity and incident response capabilities.

4. Roles and Responsibilities

Management is responsible for ensuring that appropriate security controls, procedures, and oversight mechanisms are implemented and maintained.

All personnel and authorized third parties must:

- Follow internal security procedures;
- Maintain confidentiality of sensitive information;
- Protect access credentials and devices;
- Immediately report any suspected security incident or unauthorized activity.

Access to sensitive systems and information is limited only to authorized individuals based on operational necessity.

5. Access Control

The Company applies access-control measures designed to restrict unauthorized access to systems and information.

Security measures include:

- Unique user credentials and password protection;
- Role-based access permissions;
- Restricted administrative access;
- Periodic review of user-access rights;
- Immediate revocation of access where no longer required.

Passwords and authentication credentials must remain confidential and may not be shared.

6. Data Protection and Confidentiality

The Company implements appropriate measures to protect personal, financial, operational, and regulatory data.

Sensitive information is processed only for legitimate business and regulatory purposes, including:

- Player account management;
- Payment processing;
- AML/CFT compliance;
- Responsible gaming obligations;
- Fraud prevention and security monitoring.

Confidential information may only be disclosed where legally required or authorized.

7. System and Network Security

The Company maintains technical and organizational safeguards designed to protect its infrastructure and systems from unauthorized access, misuse, disruption, or cyber threats.

Security measures may include:

- Encrypted communications;
- Firewalls and access restrictions;
- Security monitoring;
- Anti-malware protections;
- Secure administrative procedures;
- Regular software and security updates.

8. Monitoring and Incident Management

The Company monitors operational systems and may review account, transactional, or technical activity for security, fraud-prevention, AML/CFT, and regulatory purposes.

Any suspected security breach, unauthorized access, data compromise, or operational incident must be escalated internally without undue delay.

Where required by applicable law or regulatory obligations, the Company may report incidents to competent authorities.

9. Third-Party Service Providers

The Company may engage third-party providers in connection with hosting, payments, verification, security, compliance, or operational services.

Appropriate due diligence and reasonable security expectations are applied when engaging external providers.

Third parties with access to Company systems or information are expected to maintain appropriate confidentiality and security standards.

10. Business Continuity and Backup

The Company maintains reasonable operational and backup measures intended to support continuity of critical services and protection of essential data.

Backup and recovery procedures are periodically reviewed to reduce the risk of data loss or operational disruption.

11. Training and Awareness

Relevant personnel may receive periodic compliance, AML/CFT, fraud-prevention, responsible gaming, and information-security awareness guidance appropriate to their operational responsibilities.

12. Policy Review

This Policy may be reviewed and updated periodically to reflect:

- Regulatory developments;
- Operational changes;
- Security risks;
- Compliance requirements;
- Technological developments.

The latest approved version of this Policy shall remain internally available to relevant personnel and may be provided to competent authorities upon request.