INFORMATION SECURITY POLICY

Version 2.0
Effective Date: July 2026

Prepared in alignment with the Curaçao Gaming Authority Information Security Control Requirements (IG1).

1. Purpose

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

The Company is committed to maintaining an effective information security framework that protects its business operations, customers, business partners, and regulatory obligations against internal and external security threats.

This Policy has been developed in accordance with applicable Curaçao legislation, the requirements of the Curaçao Gaming Authority (CGA), AML/CFT obligations, and recognized information security principles. It reflects the Company's commitment to implementing security controls appropriate to its operational model and risk profile.

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

2. Scope

This Policy applies to:

- all information assets owned, processed, or managed by the Company;
- all information systems, applications, infrastructure, and operational environments supporting the Company's gaming operations;
- all employees, directors, contractors, consultants, and authorized third parties who access Company systems or information;
- all player, financial, regulatory, operational, and business information processed by or on behalf of the Company.

This Policy applies regardless of whether services are performed internally or through authorized third-party service providers.

3. Information Security Objectives

The Company seeks to achieve the following objectives:

- protect confidential, personal, financial, and regulatory information against unauthorized disclosure;

- preserve the integrity and accuracy of information and gaming-related records;
- ensure the continuous availability of critical systems and services;
- reduce cybersecurity risks through appropriate administrative, technical, and organizational controls;
- prevent fraud, unauthorized access, cyberattacks, and misuse of Company systems;
- support compliance with applicable legal, regulatory, licensing, AML/CFT, and responsible gaming requirements;
- maintain appropriate security governance throughout the organization;
- promote security awareness among personnel and authorized third parties;
- support business continuity and timely recovery following operational or security incidents.

4. Information Security Governance, Roles and Responsibilities

The Company is committed to maintaining an effective information security governance framework that supports the secure operation of its business, protects information assets, and ensures ongoing compliance with applicable legal and regulatory requirements.

Management has overall responsibility for the implementation, maintenance, and continuous improvement of the Company's information security framework. Management shall ensure that appropriate security controls, policies, resources, and oversight mechanisms are established to manage information security risks.

The Company shall:

- establish and maintain information security policies and supporting procedures;
- periodically assess information security risks affecting its operations;
- implement security controls proportionate to identified risks;
- review the effectiveness of implemented security measures on a regular basis;
- ensure that regulatory, legal, and contractual security obligations are met.

All employees, contractors, consultants, and authorized third parties are responsible for protecting Company information and complying with this Policy.

Personnel must:

- protect confidential and sensitive information;
- use Company systems only for authorized business purposes;
- maintain the confidentiality of authentication credentials;
- immediately report any suspected security weakness, incident, or unauthorized activity;
- comply with all applicable internal security procedures.

Access to Company systems and information shall be granted only on the basis of legitimate business need and the principle of least privilege. Access rights shall be reviewed periodically and removed promptly when no longer required.

The Company may delegate operational activities to authorized third-party service providers; however, responsibility for information security governance and regulatory compliance remains with K.I.K. Corporation B.V.

5. Asset Management

The Company shall maintain appropriate oversight of the information assets used to support its business operations and regulatory obligations.

Information assets include, but are not limited to:

- information systems and applications;
- servers and network infrastructure;
- end-user devices;
- gaming platforms and operational software;
- databases and electronic records;
- information processed or stored by authorized third-party service providers.

The Company shall maintain appropriate records of critical information assets and review them periodically to ensure they remain authorized, supported, and suitable for business use.

Only authorized hardware, software, and services may be used for Company operations. Unauthorized systems, applications, or devices that may introduce security risks shall be investigated and addressed appropriately.

Where third-party platforms, hosting providers, payment service providers, gaming suppliers, or other external service providers are used, the Company shall exercise appropriate oversight and due diligence to ensure that information security responsibilities are appropriately managed.

Information assets shall be protected throughout their lifecycle, including acquisition, use, maintenance, and retirement.

6. Access Control and Authentication

The Company shall implement appropriate logical access controls to ensure that access to information systems, applications, and data is granted only to authorized individuals based on legitimate business requirements.

Access rights shall be assigned according to the principles of **least privilege** and **need-to-know**, ensuring that users receive only the level of access necessary to perform their authorized duties.

The Company shall implement procedures governing the creation, modification, review, and removal of user accounts throughout their lifecycle.

Security controls include, where appropriate:

- unique user accounts for authorized personnel;
- role-based access permissions;
- controlled allocation of administrative and privileged accounts;
- periodic review of user access rights;
- prompt removal or suspension of access following termination of employment, contractual engagement, or change of responsibilities;
- secure authentication mechanisms appropriate to the sensitivity of the systems being accessed.

Passwords shall be maintained confidentially and shall comply with the Company's internal security requirements. Passwords must never be shared, disclosed, or reused in a manner that could compromise security.

Multi-factor authentication (MFA) shall be implemented for administrative accounts, remote access, and other critical systems where technically feasible and proportionate to operational risk.

The Company shall periodically review privileged access to ensure that elevated permissions remain appropriate, justified, and properly controlled.

Unauthorized attempts to access Company systems, information, or privileged functions are strictly prohibited and may result in disciplinary, contractual, or legal action.

7. Information Classification and Data Protection

The Company shall implement appropriate administrative, technical, and organizational measures to protect the confidentiality, integrity, and availability of information throughout its lifecycle.

Information shall be classified according to its sensitivity, business value, legal obligations, and regulatory requirements. Appropriate security controls shall be applied based on the classification of the information concerned.

Information processed by the Company may include, but is not limited to:

- player personal data;
- financial and payment information;
- AML/CFT and regulatory records;
- gaming and transaction records;
- business and operational information;
- confidential commercial information.

Access to sensitive information shall be restricted to authorized individuals whose duties require such access.

The Company shall ensure that information is collected, processed, stored, transmitted, retained, and disposed of in accordance with applicable legal, contractual, and regulatory requirements.

Appropriate safeguards shall be implemented to protect sensitive information against unauthorized access, disclosure, alteration, loss, or destruction.

Where personal or confidential information is processed by authorized third-party service providers, the Company shall take reasonable measures to ensure that such information is protected through appropriate contractual, technical, and organizational safeguards.

Information shall be retained only for as long as necessary to satisfy operational, legal, regulatory, and contractual obligations. When information is no longer required, it shall be securely deleted, destroyed, or otherwise disposed of using appropriate methods designed to prevent unauthorized recovery.

8. System Security and Vulnerability Management

The Company shall implement and maintain appropriate technical and organizational security controls to protect its information systems, networks, applications, and supporting infrastructure from unauthorized access, cyber threats, system failures, and other security risks.

Security controls may include, where appropriate:

- secure system configuration;
- network segmentation and access restrictions;
- firewalls and other perimeter security controls;
- anti-malware protection;
- encryption technologies;
- security monitoring and logging;
- secure remote administration;
- regular software, firmware, and operating system updates.

The Company shall maintain processes for identifying, assessing, and addressing information security vulnerabilities affecting its systems and services.

Security updates and software patches shall be applied within an appropriate timeframe, taking into consideration operational requirements, system criticality, vendor recommendations, and identified security risks.

Where appropriate, security vulnerabilities may be assessed through vulnerability scanning, vendor security notifications, internal reviews, or other suitable security assessment methods.

Configuration changes to critical systems shall be appropriately authorized, documented, and implemented in a controlled manner to minimize operational and security risks.

Only supported software and technologies shall be used where reasonably practicable. Where continued use of unsupported systems is necessary, appropriate compensating controls and risk mitigation measures shall be implemented.

The Company shall take reasonable measures to ensure that security controls remain effective through periodic review and continuous improvement.

9. Security Monitoring, Logging and Incident Response

The Company shall maintain appropriate monitoring and logging processes to support the protection of its information systems, the detection of security events, and compliance with applicable legal and regulatory obligations.

Security-related events may be monitored through appropriate technical and organizational measures designed to identify unauthorized access, suspicious activity, system failures, fraud attempts, and other events that may affect the confidentiality, integrity, or availability of Company information or services.

Where appropriate, audit logs shall be generated and retained to support operational monitoring, security investigations, regulatory compliance, and forensic analysis. Access to security logs shall be restricted to authorized personnel.

The Company shall maintain procedures for identifying, assessing, managing, and responding to actual or suspected information security incidents.

All employees, contractors, and authorized third parties are required to report suspected security incidents, vulnerabilities, or unauthorized activities without undue delay through the Company's established reporting channels.

Where a security incident may affect player data, financial transactions, gaming integrity, operational continuity, or regulatory compliance, the Company shall take appropriate measures to investigate, contain, mitigate, and document the incident.

Where required by applicable law or regulatory obligations, the Company shall notify the Curaçao Gaming Authority and any other competent authority within the applicable regulatory timeframes.

Following significant security incidents, the Company shall review the effectiveness of its response and implement corrective actions where appropriate to reduce the likelihood of recurrence.

10. Third-Party Information Security

The Company may engage authorized third-party service providers to support various aspects of its business operations, including gaming platforms, payment processing, hosting, software development, identity verification, security services, compliance functions, and other operational activities.

Although certain operational functions may be performed by third parties, K.I.K. Corporation B.V. remains responsible for ensuring that appropriate information security measures are maintained in accordance with applicable legal and regulatory requirements.

Prior to engaging a third-party service provider, the Company shall perform reasonable due diligence appropriate to the nature of the services provided and the information or systems to which the provider may have access.

Where appropriate, contractual arrangements with third-party providers shall include provisions relating to:

- confidentiality and protection of information;
- information security responsibilities;
- compliance with applicable legal and regulatory requirements;
- incident notification where security events may affect Company operations or regulated information;
- protection of personal and confidential information.

The Company shall periodically review third-party relationships and take reasonable measures to ensure that service providers continue to maintain appropriate security standards throughout the duration of the engagement.

Where third-party providers process, store, or transmit Company or player information, appropriate safeguards shall be maintained to protect the confidentiality, integrity, and availability of such information.

The Company shall maintain appropriate oversight of outsourced activities and shall not rely solely on contractual arrangements to satisfy its regulatory responsibilities.

11. Business Continuity, Backup and Recovery

The Company is committed to maintaining the resilience and continuity of its critical business operations and information systems in the event of operational disruption, cybersecurity incidents, system failures, or other unforeseen events.

Appropriate business continuity and disaster recovery measures shall be maintained to support the timely recovery of critical services and minimize the impact of operational interruptions.

The Company shall implement appropriate backup procedures for critical information, systems, and business records to support data availability and recovery where required.

Backup data shall be protected against unauthorized access, alteration, loss, or destruction through appropriate technical and organizational safeguards.

Recovery procedures shall be periodically reviewed and tested where appropriate to ensure that critical business functions can be restored within reasonable timeframes.

Business continuity planning shall take into consideration the Company's operational model, reliance on authorized third-party service providers, regulatory obligations, and the protection of player information and gaming operations.

Where significant operational or technological changes occur, the Company shall review the adequacy of its business continuity and recovery arrangements and implement improvements where necessary.

12. Security Awareness and Human Resources

The Company recognizes that information security depends not only on technical controls but also on the awareness, competence, and responsible conduct of its personnel.

Employees, contractors, consultants, and other authorized individuals with access to Company information or systems are expected to understand and comply with their information security responsibilities.

The Company shall promote information security awareness through appropriate guidance, communication, and periodic training relevant to employees' roles and responsibilities.

Where appropriate, personnel shall receive training covering topics including:

- information security responsibilities;
- protection of confidential information;
- password and authentication practices;
- phishing and social engineering awareness;
- secure handling of Company and player information;
- incident identification and reporting;
- applicable regulatory and compliance obligations.

Personnel with access to sensitive information or critical systems are expected to exercise an appropriate standard of care in protecting Company assets and complying with internal security requirements.

The Company may implement appropriate measures throughout the employment or engagement lifecycle, including confidentiality obligations, controlled access to systems, and the timely removal of access rights when employment or contractual relationships end.

Failure to comply with this Policy or other applicable information security requirements may result in appropriate disciplinary, contractual, or other corrective action.

13. Compliance, Governance and Continuous Improvement

The Company is committed to maintaining an effective information security governance framework that supports compliance with applicable legal, regulatory, contractual, and business requirements.

Information security shall be integrated into the Company's overall governance, risk management, and operational decision-making processes.

The Company shall periodically assess information security risks and implement appropriate controls designed to reduce identified risks to an acceptable level, taking into consideration the Company's operational model, regulatory obligations, and evolving threat landscape.

Management shall oversee the implementation of this Policy and shall promote a culture of continuous improvement through the regular evaluation of security controls, operational practices, and compliance activities.

The Company shall monitor changes to applicable legislation, regulatory requirements, industry standards, and business operations to ensure that its information security framework remains appropriate and effective.

Where deficiencies, vulnerabilities, or opportunities for improvement are identified through internal reviews, security incidents, audits, regulatory assessments, or operational experience, appropriate corrective actions shall be implemented.

The Company shall cooperate with competent regulatory authorities and maintain appropriate documentation demonstrating its commitment to information security and regulatory compliance.

14. Policy Review, Approval and Document Control

This Policy shall be reviewed periodically, and at least annually, or whenever significant legal, regulatory, operational, or technological changes occur.

The Policy may also be reviewed following significant information security incidents, regulatory findings, internal audits, or material changes to the Company's operational environment.

Management is responsible for approving this Policy and any subsequent revisions.

The current approved version of this Policy shall be maintained as a controlled document and made available to relevant personnel. Previous versions shall be retained in accordance with the Company's document management practices.

This Policy becomes effective upon approval by Management and remains in force until amended or replaced.

Version	Date	Description
1.0	May 2026	Initial Information Security Policy
2.0	July 2026	Updated to align with the CGA Information Security Control Requirements (IG1 Consultation Version)