

INFORMATION SECURITY POLICY

Apex Gaming International N.V.

B2B Gaming Supplier

Version: 1.0

Effective Date: May 5, 2026

Approved By: Managing Director / Board of Directors

Review Frequency: Annual or upon material operational or regulatory changes

1. Introduction

This Information Security Policy ("Policy") establishes the information security framework of Apex Gaming International N.V. (the "Company"), a B2B supplier operating within the gaming industry.

The purpose of this Policy is to ensure the confidentiality, integrity, and availability of the Company's information assets, systems, infrastructure, software, operational processes, and business data in accordance with the requirements and expectations of the Curaçao Gaming Authority ("CGA"), the National Ordinance on Games of Chance (LOK), applicable AML/CFT obligations, and recognized international information security standards.

As a B2B supplier, the Company provides services and/or technology solutions to licensed operators and business partners and recognizes the importance of maintaining secure and resilient systems capable of supporting regulated gaming operations.

This Policy applies to all directors, employees, contractors, consultants, and third-party service providers acting on behalf of the Company or accessing Company systems, networks, or information.

2. Information Security Objectives

The Company is committed to implementing and maintaining appropriate technical and organizational measures to protect its operational environment from cybersecurity threats, unauthorized access, data compromise, fraud, operational disruption, and misuse of confidential information.

The primary objectives of this Policy are to:

- maintain the security and resilience of Company systems and services;
 - protect confidential business, operational, technical, and regulatory information;
 - support secure B2B service delivery to operators and business partners;
 - minimize operational and cybersecurity risks;
 - ensure business continuity and operational stability; and
 - support compliance with applicable regulatory and contractual obligations.
-

3. Governance & Responsibilities

Senior management of Apex Gaming International N.V. is responsible for overseeing the implementation and maintenance of this Policy and ensuring that appropriate information security measures are integrated into the Company's operations.

Management shall ensure that sufficient resources, procedures, and internal controls are maintained to support cybersecurity, operational security, incident management, and regulatory compliance.

The designated Information Security Officer, Compliance Officer, or responsible personnel shall oversee the day-to-day administration of information security matters, monitor compliance with this Policy, coordinate incident response activities, and periodically assess security-related risks.

All personnel are responsible for protecting Company systems, credentials, and confidential information and must comply with the requirements set forth in this Policy. Any suspected security incident, weakness, or unauthorized activity must be reported immediately to management or designated responsible personnel.

4. Information Classification & Confidentiality

The Company shall maintain appropriate safeguards for all information processed, transmitted, or stored within its operational environment.

Information may be classified according to its sensitivity and operational importance. Sensitive information may include:

- business and commercial information;
- operator-related information;
- platform and technical documentation;
- authentication credentials;
- financial information;
- AML/KYC-related records;
- regulatory communications; and
- internal operational documentation.

Access to confidential information shall be limited strictly to authorized individuals whose responsibilities require such access.

Appropriate safeguards, including encryption and restricted access controls, shall be implemented where necessary to protect sensitive information against unauthorized disclosure, modification, or misuse.

5. Access Control & User Management

Access to Company systems and infrastructure shall be granted based on the principles of least privilege and business necessity.

Each authorized user shall utilize unique login credentials. Password requirements shall follow internal security standards designed to reduce unauthorized access risks.

Multi-factor authentication (MFA) shall be implemented for critical systems, administrative accounts, cloud environments, remote access solutions, and other systems deemed sensitive by management.

User access rights shall be periodically reviewed to ensure continued appropriateness. Access privileges shall be revoked promptly following termination of employment, contractual relationship, or changes in responsibilities.

Administrative access to production environments, infrastructure, and sensitive systems shall be restricted to specifically authorized personnel only.

6. Infrastructure & Network Security

The Company shall maintain appropriate technical safeguards designed to protect its infrastructure, systems, software environments, and operational networks.

Security controls may include firewalls, endpoint protection, anti-malware solutions, intrusion detection or prevention systems, network segmentation, monitoring systems, secure remote access mechanisms, and vulnerability management procedures.

Systems and software shall be updated regularly through patch management procedures intended to address known vulnerabilities and maintain operational stability.

Logging and monitoring mechanisms shall be maintained to identify suspicious activities, unauthorized access attempts, operational anomalies, and potential cybersecurity incidents.

7. Operational Security & Software Management

As a B2B supplier, the Company recognizes the importance of maintaining secure and reliable operational systems and software environments.

Where software development, integrations, or system modifications are performed internally or through third-party providers, appropriate testing, validation, and approval procedures shall be followed prior to deployment into production environments.

Critical system changes shall be documented and approved by authorized personnel before implementation.

Where feasible, development, testing, and production environments shall remain appropriately segregated to reduce operational and security risks.

8. Third-Party Providers & Outsourcing

The Company may engage third-party providers for infrastructure hosting, cloud services, cybersecurity solutions, software development, AML/KYC tools, communication systems, or other operational support services.

Appropriate due diligence shall be conducted prior to onboarding critical third-party providers to assess their suitability, reliability, and security posture.

Third-party providers may be required to comply with confidentiality obligations and applicable security requirements established by the Company.

Management reserves the right to periodically review critical outsourced services and providers where necessary from an operational, compliance, or security perspective.

9. Incident Management & Reporting

The Company shall maintain procedures for identifying, managing, documenting, and responding to information security incidents.

Security incidents may include unauthorized access attempts, malware infections, phishing attacks, infrastructure failures, service disruptions, denial-of-service attacks, credential compromise, or any event capable of affecting the confidentiality, integrity, or availability of Company systems or information.

All personnel must immediately report suspected or confirmed incidents to management or designated responsible personnel.

The Company shall investigate incidents in a timely manner and implement corrective measures where necessary to minimize operational impact and reduce the likelihood of recurrence.

Where required under applicable laws, regulations, or directives issued by the Curaçao Gaming Authority, reportable incidents shall be escalated and reported accordingly.

10. Business Continuity & Disaster Recovery

The Company shall maintain reasonable business continuity and disaster recovery measures to support operational resilience and continuity in the event of cyber incidents, infrastructure failures, operational disruptions, or other emergencies.

Backup procedures shall be implemented for critical systems, configurations, and operational data. Backup information shall be protected appropriately and periodically tested where feasible.

The Company shall maintain recovery procedures intended to restore critical systems and services within reasonable timeframes following an operational disruption or security incident.

Management may periodically review continuity and recovery procedures to assess effectiveness and operational readiness.

11. Physical Security

Appropriate physical security measures shall be implemented to protect Company offices, infrastructure, devices, systems, and confidential information against unauthorized physical access, theft, damage, or interference.

Access to restricted operational areas and infrastructure environments shall be limited to authorized personnel only.

Confidential physical documentation shall be stored securely and disposed of appropriately when no longer required.

12. Security Awareness & Training

The Company recognizes that effective information security requires ongoing awareness and responsible conduct by all personnel.

Employees and relevant contractors shall receive periodic information security and cybersecurity awareness training appropriate to their operational responsibilities.

Training may include cybersecurity awareness, phishing prevention, password security, secure handling of confidential information, operational security procedures, and incident reporting obligations.

13. Monitoring, Review & Compliance

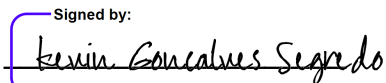
The Company may conduct periodic internal reviews, assessments, or audits to evaluate compliance with this Policy and the effectiveness of implemented security controls.

This Policy may be updated from time to time to reflect operational changes, evolving cybersecurity threats, technological developments, contractual obligations, or updated requirements issued by the Curaçao Gaming Authority or other competent authorities.

Failure to comply with this Policy may result in disciplinary action, restriction of access privileges, termination of contractual relationships, or further action where appropriate.

14. Policy Approval

Approved on behalf of Apex Gaming International N.V.

Signed by:

FE5E1D081F9148D...

Name: Elite Management B.V.

Title: Managing Director

Date: May 5, 2026