

Information Security Policy - Kanggiten B.V

INFORMATION SECURITY POLICY

Effective Date: February 2025

Ver 1.1

1. INTRODUCTION AND SCOPE

1.1 Purpose

This Information Security Policy (ISP) sets forth a methodical approach, based on the ISO/IEC 27001 framework, for securing all information assets. It establishes administrative, physical, and technical controls to protect the Confidentiality, Integrity, and Availability (CIA) of data belonging to Kanggiten B.V, a company registered in Curacao, with company number 147119, with registered address Korporaalweg 10, Willemstad, Curacao (Company) and its Counterparties (B2B Operators and Game Providers). The priority is securing B2B integration points and maintaining game integrity.

1.2 Scope

This Policy is a mandatory standard for all personnel and third parties and applies to:

- ✓ The Game Aggregation Platform (GAP), Remote Gaming Server (RGS) communication links, B2B APIs, and all supporting back-office systems.
- ✓ All data processed, including proprietary IP (source code), player transactional data, and confidential B2B partner information.
- ✓ All network infrastructure and physical facilities owned or used by the Company in its Curaçao operations.

1.3 Legal and Regulatory Framework

This Policy aligns with:

- ✓ GDPR: Compliance with Regulation (EU) 2016/679 (Article 32).
- ✓ Curaçao Licensing Requirements: Adherence to all security and operational requirements mandated by the licensing authority, particularly concerning RGS integrity, fraud prevention, and transaction logging.

- ✓ ISO/IEC 27001: Provides the structural foundation for the Information Security Management System (ISMS).

2. GOVERNANCE AND RISK MANAGEMENT

2.1 Information Security Principles

The security program ensures:

- ✓ Confidentiality: Protecting sensitive B2B data (API keys, partner specifications) and player financial data.
- ✓ Integrity: Ensuring the accuracy of RNG data, game logic, transaction records, and financial reports.
- ✓ Availability: Guaranteeing high uptime for the Game Aggregation Platform to support 24/7 B2B operations.

2.2 Risk Management

The Company utilizes a formal, systematic risk management process:

- ✓ Risk Assessment: Annual risk assessments are mandatory, covering threats to the B2B API infrastructure (e.g., unauthorized access, service attacks, configuration errors) and potential regulatory non-compliance.
- ✓ Risk Treatment: Risks identified must be mitigated, transferred, avoided, or formally accepted by Executive Management in a documented Risk Treatment Plan.

3. SECURITY ORGANISATION AND PERSONNEL SECURITY

3.1 Internal Security Organisation

The Information Security Officer (ISO) is responsible for leading the ISMS, managing security operations, and ensuring policy enforcement.

3.2 Personnel Security

The Principles of Personnel Security	
Pre-Employment	Background screening is mandatory for personnel with access to critical B2B production systems.

Training and Awareness	Security awareness training must include specific modules on API key handling, phishing threats targeting B2B credentials, and regulatory obligations.
Termination	All system and B2B partner access must be revoked immediately upon departure.

4. ASSET MANAGEMENT

4.1 Asset Classification and Inventory

All information assets are categorized. Assets related to B2B integrations are categorized as Confidential (Proprietary source code, integration specifications, partner API keys, and sensitive financial models). These assets require the highest level of protection.

4.2 Media Handling

Secure procedures must be followed for the storage, transfer, and disposal of physical and digital media. Confidential information must not be stored on unauthorized or unencrypted portable devices.

5. ACCESS CONTROL

Access control is governed by the principles of “Least Privilege” and “Need-to-Know”:

5.1 User Access Management

- ✓ Authentication: Multi-Factor Authentication (MFA) is mandatory for all administrative and operational accounts with access to the Game Aggregation Platform and partner data.
- ✓ Password Policy: Must adhere to the Password Policy, requiring minimum complexity (e.g., minimum 12 characters, non-reusable) and regular rotation.

5.2 External B2B Access and Key Management (Critical Technical Control)

- ✓ Unique Credentials: Each B2B Counterparty must be issued a unique, separate set of credentials (API keys, secrets).
- ✓ Secure Storage: All API keys and secrets (both internal and external) must be stored in an approved, centrally managed secrets management vault and must not be hardcoded or stored in plain text configuration files.

- ✓ API Validation: All B2B API requests must be validated for authenticity, including cryptographic signing, timestamp verification, and source IP whitelisting.

6. TECHNICAL SECURITY CONTROLS

6.1 Network Security and Segmentation

- ✓ Segregation: Critical B2B systems (RGS links, production databases) must be logically and physically segmented from the corporate network, development, and testing environments.
- ✓ Firewalls: Firewalls are configured on a default-deny policy. External endpoints must be protected by perimeter firewalls and Web Application Firewalls (WAFs) to filter traffic and defend against application-layer attacks (e.g., injection, DoS).
- ✓ Remote Access: All remote access to the internal network (including B2B back-offices) must utilize approved, encrypted VPN tunnels.
- ✓ Intrusion Detection/Prevention (IDS/IPS): IDS/IPS systems must be deployed to monitor network traffic for malicious patterns indicative of attempts to compromise B2B communication channels.

6.2 Cryptographic Controls

- ✓ Data in Transit (B2B API): All B2B API communications must use TLS 1.2 or higher and must enforce strong cipher suites. Older or insecure protocols are prohibited.
- ✓ Data at Rest (Disk and Database Encryption): Sensitive databases (including transaction logs and player data) and production server volumes must be encrypted at rest using industry-standard, strong cryptographic algorithms (e.g., AES-256).

6.3 Secure Development and Application Security (SSDLC)

- ✓ Secure Design: All new B2B features and integrations must undergo a formal security review and threat modeling process.
- ✓ Input Validation: Mandatory, rigorous input and output validation across all API endpoints to prevent injection, tampering, and ensure the integrity of game commands and financial transactions.
- ✓ Code Review: Mandatory security-focused code reviews for all production

deployments.

- ✓ Vulnerability Scanning: Use of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools is mandatory during the development lifecycle.

6.4 Patch and Vulnerability Management

- ✓ Patching SLA: Critical vulnerabilities (CVSS 9.0+) must be patched or mitigated within 7 days of vendor release. High-risk vulnerabilities within 30 days.
- ✓ Anti-Malware: Anti-malware and Endpoint Detection and Response (EDR) solutions are mandatory on all endpoints and servers.

7. IT OPERATIONS MANAGEMENT

7.1 Change Management

- ✓ All changes affecting the security of the Game Aggregation Platform or B2B connections must be managed through a formal Change Management Process, including peer review, testing in a non-production environment, and documented approval by the ISO.

7.2 Logging, Monitoring, and Auditing

- ✓ Centralized Logging: Logs from all critical B2B and production systems (APIs, RGS links, Databases, Firewalls) must be securely collected, timestamped, and stored in a central, tamper-proof repository.
- ✓ Mandatory Logs: Logs must explicitly capture: all B2B authentication failures, API access attempts, system configuration changes, and game transaction errors/anomalies to ensure compliance with Curacao requirements.
- ✓ Log Retention: Logs must be retained for a minimum of 6 months, or longer if mandated by regulation.

7.3 Backups and Disaster Recovery

- ✓ Backup Integrity: Regular, tested backups are mandatory. A copy of the backup must be stored off-site and encrypted.
- ✓ DR Plan: The Disaster Recovery Plan must be tested annually to ensure that critical B2B services can be restored within defined RTO/RPO targets

8. THIRD-PARTY SECURITY (B2B PARTNERSHIPS)

8.1 Onboarding and Assessment

New B2B partners (Game Providers and Operators) must complete a security questionnaire and undergo an initial security assessment to confirm minimum security standards before integration.

8.2 Contractual Requirements

All B2B agreements must contain explicit security clauses addressing data protection, liability, mandatory breach notification periods, and the right to audit the partner's systems relating to the integration point.

9. INCIDENT RESPONSE AND COMPLIANCE

9.1 Incident Management

The Company maintains an Incident Management Process Policy covering the entire lifecycle of a security incident.

- ✓ Reporting: All suspected incidents (e.g., API abuse, platform downtime) must be reported immediately to the ISO.
- ✓ Response: Incidents are classified based on the risk to game integrity and business impact. The response includes containment, eradication, and system recovery.

9.2 Breach Notification

In case of a Personal Data Breach, notification procedures (including those to the Supervisory Authority and B2B Counterparties) will follow the timelines set forth in the

Data Protection Policy.

9.3 Policy Compliance and Audit

- ✓ Internal Audits: Internal security audits are conducted at least annually.
- ✓ External Audits: Mandatory annual external penetration testing of the B2B API/GAP infrastructure is required for licensing compliance.

10. POLICY ENFORCEMENT

10.1 Violations

Violations of this Policy by personnel may result in disciplinary action, up to and including termination. Violations by B2B Counterparties may lead to immediate suspension of access and termination of the service agreement.

11. REVISIONS OF THIS POLICY

11.1 Revision

This Policy is subject to revision each year. In addition, this Policy may be revised in the following cases:

- ✓ Changes in applicable data protection legislation;
- ✓ Changes in the corporate structure of the Company;
- ✓ Changes in the business profile of the Company;
- ✓ There are found sufficient deficiencies of this Policy or Company's data protection rules;
- ✓ In other cases when the situation may require a revision of the document.