

Information Security Policy (ISP) – Curaçao Gaming Board (GCB) Compliance

1. Policy Overview and Regulatory Commitment

1.1. Purpose

This Information Security Policy (ISP) establishes the mandatory controls and standards necessary to protect the Confidentiality, Integrity, and Availability (CIA) of all information assets used in connection with the organization's online gaming operations.

1.2. Scope

This policy applies to all employees, contractors, third-party suppliers, systems, networks, and data (including player data and transactional history) that support the iGaming activities licensed and regulated by the Curaçao Gaming Board (GCB) / Curaçao Gaming Authority (CGA).

1.3. GCB Regulatory Compliance Mandates

The policy is designed to align with GCB/CGA requirements, specifically concerning:

1. System and Game Integrity: Ensuring the fairness and reliability of all gaming software (Section 4).
2. Player Protection and KYC/AML: Securing sensitive player data and transactional records (Section 5).
3. Physical and Logical Security: Maintaining appropriate control over infrastructure, including local presence requirements (Section 6).
4. Auditing and Reporting: Establishing mechanisms for independent verification and incident reporting (Section 7).

2. Governance and Organization of Information Security

2.1. Security Roles and Responsibilities

Roles and responsibilities for information security are clearly defined to ensure accountability:

- Board/Management: Responsible for final approval and funding of the ISP and determining overall risk tolerance.
- Chief Information Security Officer (CISO): Responsible for the creation, implementation, maintenance, and enforcement of this ISP. Acts as the primary liaison for GCB security audits.
- System Administrators: Responsible for the implementation of technical controls, patch management, and monitoring of system logs.
- All Employees: Responsible for mandatory adherence to the ISP and immediate reporting of security incidents to the CISO.

2.2. Segregation of Duties (SoD)

Critical operational tasks must be segregated. Specifically:

- Developers shall not have direct access to production deployment or configuration.

- Financial transaction approval shall be separate from transaction logging.
- System administrators shall not have access to player personally identifiable information (PII) beyond what is required for maintenance.

3. Asset and Risk Management

3.1. Asset Inventory

A comprehensive and up-to-date inventory of all hardware, software, licenses, and data repositories must be maintained. This inventory must clearly identify all critical gaming system components (RNG, Game Server, Payment Gateways, Player Database).

3.2. Risk Assessment

Formal risk assessments must be conducted at least annually, and whenever significant changes occur (e.g., new game provider integration, infrastructure migration). The assessment shall focus on threats to game integrity, player data, and financial transactions.

4. Technical Compliance and Game Integrity

4.1. Certified Software and RNG

- **Mandate:** All gaming software, including the Random Number Generator (RNG) used for games of chance, must be tested and certified by an accredited, independent testing laboratory (ITL) approved by the GCB/CGA.
- **Verification:** Proof of certification must be stored securely and made available to the GCB/CGA upon demand.
- **Change Control:** Any changes to certified gaming logic or the RNG algorithm must be formally logged, approved, and re-certified before deployment to the production environment.

4.2. Network Security and Configuration

- **Firewalls:** Perimeter firewalls and internal network segmentation must be deployed to separate the production gaming environment from the corporate network.
- **Vulnerability Management:** All servers and applications must undergo regular vulnerability scanning. Critical patches must be applied within seven (7) days of release.
- **Configuration Hardening:** All operating systems, network devices, and databases must be configured according to industry-standard hardening guides (e.g., CIS Benchmarks).

5. Data Protection, KYC, and AML/CFT Security

5.1. Data Encryption (Mandatory)

Data must be protected based on its state:

- Data in Transit:

- Requirement: All player-facing communications (login, betting, financial transactions, document upload) must be secured.
- Minimum Standard: TLS 1.2 or higher, using strong ciphers.
- Data at Rest:
 - Requirement: All critical player data (PII, passwords, payment details, transaction history, KYC documents) must be encrypted when stored on disk.
 - Minimum Standard: AES-256 or equivalent.

5.2. Access Control and Authentication

- Authentication: Multi-Factor Authentication (MFA) is mandatory for all administrative access to production systems, player databases, and financial systems.
- Passwords: Strong password policies (minimum 12 characters, complexity requirements) must be enforced for all user and system accounts.
- Principle of Least Privilege: Access rights are granted strictly on a "need-to-know" and "need-to-use" basis.

5.3. Protection of AML/KYC Data

- Confidentiality: Documents collected for Know Your Customer (KYC) and Customer Due Diligence (CDD) must be stored in a segregated, encrypted repository with highly restricted access.
- Retention: Data retention must comply with the GCB/CGA's mandate regarding AML/CFT record-keeping.

6. Physical and Environmental Security (Curaçao Presence)

6.1. Local Server Requirement

As mandated by the GCB/CGA, at least one physical gaming server or approved infrastructure component hosting critical regulatory data (player register, transaction logs) must be located within the jurisdiction of Curaçao.

6.2. Physical Access Control

- The facility housing the Curaçao-based server(s) must implement robust physical security controls, including:
 - 24/7 Monitoring and surveillance (CCTV).
 - Multi-factor access control (e.g., badge + biometric).
 - Visitor logs must be maintained for GCB inspection.

6.3. Media Handling and Disposal

All storage media containing sensitive data must be securely sanitized or physically destroyed prior to disposal or reuse, following industry-standard methods (e.g., NIST SP 800-88).

7. Business Continuity, Incident Management, and Auditing

7.1. Backup and Disaster Recovery (DRP)

- Backup Strategy: Full and incremental backups of all critical data (including the player database, game logs, and transaction history) shall be performed regularly and stored securely, with at least one off-site copy.
- DRP Testing: A formal Disaster Recovery Plan (DRP) must be maintained, and recovery procedures must be tested at least once per year to ensure the gaming system can be restored within a designated timeframe (RTO/RPO).

7.2. Incident Response Plan (IRP)

A documented IRP must be in place to handle security incidents, breaches, and system failures.

The IRP must mandate:

- Immediate isolation and containment of affected systems.
- Detailed forensic logging and preservation of evidence.
- Mandatory GCB Notification: The CISO must immediately notify the GCB/CGA of any material security incident, data breach, or loss of game integrity, in accordance with the Authority's specified timelines.

7.3. Mandatory Independent Audits

- Frequency: The organization's compliance with this ISP and the GCB/CGA regulations shall be subject to independent third-party audit and penetration testing at least annually.
- Reporting: Audit reports, penetration test findings, and the management's plan to remediate any identified weaknesses must be submitted to the GCB/CGA.

November 14, 2025