

Operational Manual

SXM Management N.V.

Groot Kwartierweg 10

Livestrong Building

Curacao

Curacao License Number: OGL/2024/7777/0364

Table of Contents:

1. Introduction
2. Business Overview
3. Payment Service Providers (PSPs)
4. Software and Platform Infrastructure
5. Random Number Generator (RNG) and Fair Gaming
6. Quality Assurance and Testing
7. Information Security Policy
8. IT Resources and Infrastructure
9. Data Uploading, Storage, and Protection
10. Applications and Security Measures
11. Contact Information

1. Introduction

This Operational Manual sets out policies, technical framework, and procedures to ensure operational integrity, system security, and compliance with the Curaçao licensing framework.

Operations are conducted under a dual model:

- B2C Operations, offering online gaming services in permitted (.com) markets, strictly limited to non-restricted jurisdictions.

The platform does not develop games of chance, operate RNG systems, or process cardholder data. Instead, it provides the secure infrastructure and integrations necessary to support operators and players.

2. Business Overview

Operations cover below business line:

1. B2C Operations

- Active under a Curaçao license in .com markets, limited strictly to non-restricted jurisdictions.
- Online casino and sportsbook services provided through third-party providers integrated via the platform.
- Payments processed through PSP integrations; no sensitive cardholder data is stored or processed internally.

Responsibilities and Scope

- Game Providers: Supply RNG-based content. Certifications are requested and maintained where provided.
- Third-Party Vendors (CRM, Affiliate, etc.): Integrated into the platform; security and technical alignment validated.
- Operators: Responsible for AML/KYC obligations in line with Curaçao regulations (customer identification, monitoring, and reporting of unusual transactions).
- Platform: Provides infrastructure, manages integrations, and ensures alignment with Curaçao licensing requirements.

3. Payment Service Providers (PSPs)

The platform integrates with multiple PSPs to enable secure payment processing for operators and B2C operations in non-restricted (.com) markets.

- **PSP Selection**
PSPs are chosen based on availability in target markets.
- **Data Handling**
No cardholder data is stored, processed, or transmitted within the platform. All sensitive data is handled directly by PSPs.
- **Integration and Security**
 - Secure API and HTTPS protocols for all PSP integrations.
 - Transactional information (excluding sensitive data) logged for reconciliation and monitoring.
 - Technical and functional validations performed before deployment.
- **Flexibility**
No fixed PSP list is published; integrations depend on market and business requirements.

4. Software and Platform Infrastructure

- **Core Platform**
 - Player Account Management (PAM)
 - Back-office administration and reporting
 - Risk and transaction monitoring modules
- **Integrated Systems**
 - Casino Engine for casino provider integrations
 - MOP for sportsbook provider integrations
 - CRM and Affiliate systems via third-party vendors
 - Payment gateway modules for PSP connections
- **Hosting & Cloud Services**
 - Hosted on secure on-prem and cloud infrastructure with redundancy and failover mechanisms.
 - Continuous monitoring with uptime aligned to industry standards.

- Scalability
Modular design enables new integrations without disruption.

5. Random Number Generator (RNG) and Fair Gaming

The platform does not develop or operate RNG systems. All content is provided by third-party providers.

- RNG Certification
 - Certifications requested during onboarding.
 - Documents provided are archived and maintained.
- Transparency
 - Certification documentation is stored and can be presented to regulators on request.

6. Quality Assurance and Testing (6 to 10 To be checked by the IT Team)

Quality assurance is embedded into the development and release cycle.

- Scope
 - Platform functionality and performance
 - Third-party integrations (casino, sportsbook, CRM, Affiliate, PSP)
 - Load and performance tests during development cycles
- Approach
 - QA testing performed during development and before weekly releases.
 - Stress/load tests run for major updates or where required.
- External Audits
 - Conducted when required by regulation or business needs.
- Issue Management
 - Issues logged, prioritized, and resolved within development cycles.

7. Information Security Policy

- Access Control
Role-based access, MFA, and regular access reviews.
- Encryption
TLS 1.2/1.3 for data in transit.
- Incident Management
Procedures for detection, reporting, and mitigation.
- Monitoring & Logging
Secure log collection and anomaly detection.
- Employee Awareness
Security awareness initiatives provided to staff.
- Third-Party Integrations
Security assessments conducted for all vendor connections.

8. IT Resources and Infrastructure

- Hardware & Cloud Resources
Redundant on-prem and cloud servers, secure workstations, and networking devices.
- Software
Licensed OS, monitoring tools, firewalls, and endpoint security.
- Network Security
Firewalls, VPNs, IDS/IPS, and segregated environments (dev/stage/prod).
- Maintenance & Monitoring
Regular patching, upgrades, and continuous server monitoring.

9. Data Uploading, Storage, and Protection

- Uploading
Secure transfer protocols (SFTP, HTTPS).
- Storage
No cardholder data stored. Operational data encrypted in databases.
- Protection
Stored in isolated network segments, TLS in transit. Access logging enforced.
- Backup & Recovery
Automated daily backups with off-site storage.

- Privacy Compliance
Alignment with Curaçao regulations and international best practices.

10. Applications and Security Measures

- Applications
 - PAM system
 - PSP gateway modules
 - CRM and Affiliate via 3rd party vendors
 - Casino Engine for provider integrations
 - Trading Application (Sportsbook) with in-house fraud and player monitoring
 - Casino fraud checks handled by game providers directly
- Security Measures
 - WAF and secure coding
 - Strong session management
 - Vulnerability scans and penetration testing
 - Structured change control and QA before releases
 - Continuous monitoring of performance and transactions

11. Compliance and Continuous Improvement: (To be completed by the Compliance Team)

- Regulatory Compliance:
Regular audits to ensure adherence to Curacao gaming laws and AML/KYC regulations.
- Training & Development:
Ongoing