

INFORMATION SECURITY POLICY

REVISION HISTORY

Version Number	Date	Summary of changes	Author
1.0	01/05/2025	New policy drafted	Edward Mackrill
1.1	01/03/2026	Updated in line with CGA guidance	Edward Mackrill

Approved by: Gouloud Hammoud, Director	
---	--

PURPOSE

This Information Security Policy & Framework defines how **JMS Investment Group N.V.** ("**the Company**") protects its information assets, systems, and data.

The objectives are to:

- Ensure compliance with **Curaçao Gaming Authority (CGA)** requirements
- Protect player data, financial information, and operational systems
- Mitigate cyber and operational risks
- Establish a structured **Information Security Management Framework (ISMF)**

This policy is supported by operational documentation, including the **Information Security Risk Register (Appendix A)** and **Incident Log (Appendix B)**.

SCOPE

This policy applies to:

- All employees, contractors, and third parties
- All systems used to process, store, or transmit Company or player data
- All environments, including remote working

INFORMATION SECURITY PRINCIPLES

The Company adheres to:

- **Confidentiality** – Data is accessible only to authorised individuals
- **Integrity** – Data is accurate and protected from unauthorised modification
- **Availability** – Systems and data are accessible when required

GOVERNANCE & RESPONSIBILITIES

Board of Directors

- Ultimate accountability for information security
- Approves policies and risk appetite

Key Compliance Function (KCF)

- Ensures compliance with CGA requirements
- Oversees incident reporting and regulatory communication

Information Security / IT Function

- Implements and maintains security controls
- Monitors systems, threats, and vulnerabilities

All Personnel

- Must comply with this policy
- Must report any suspected incidents immediately

CYBER RISK MANAGEMENT FRAMEWORK

The Company adopts a **risk-based approach** to information security.

Risk Assessment

- Risks are identified across:
 - Data protection
 - Platform security
 - Payments and fraud

- Third-party dependencies
- Risks are assessed using a **Likelihood × Impact methodology**

Risk Register

- A formal **Information Security Risk Register** is maintained by the KCF and reviewed with senior management (see **Appendix A**):
 - At least annually
 - Upon significant system or business changes

Risk Treatment

- Risks are:
 - Mitigated through controls
 - Accepted with documented rationale
 - Avoided where necessary

ACCESS CONTROL POLICY

Principles

- **Least privilege access**
- **Role-Based Access Control (RBAC)**

Authentication

- Multi-Factor Authentication (MFA) is required for:
 - Administrative access
 - Back-office systems
 - Payment systems

User Lifecycle Management

- **Joiners:** Access granted based on management approval
- **Movers:** Access adjusted according to role changes
- **Leavers:** Access revoked immediately (within 24 hours maximum)

Access Reviews

- Conducted at least **every 6 months**

Privileged Access

- Restricted to authorised personnel
- Subject to monitoring and logging

DATA PROTECTION & CLASSIFICATION**Data Classification**

- Public
- Internal
- Confidential
- Highly Confidential (Player & Financial Data)

Protection Measures

- Data must be protected using:
 - Encryption in transit (TLS 1.2+)
 - Encryption at rest (e.g. AES-256)
- Access restricted based on role
- Sensitive data must not be stored unencrypted on local devices

SYSTEM AND NETWORK SECURITY

- Firewalls and network controls are implemented
- Secure VPN is required for administrative access
- Production and development environments are segregated
- Systems are regularly patched and monitored

APPLICATION SECURITY

- Secure development practices are followed
- Passwords must be:
 - Hashed and salted
 - Non-reversible
- Player sessions must include:
 - Timeout controls
 - Protection against unauthorised access

LOGGING AND MONITORING

- Logs are maintained for:
 - User access
 - Administrative actions
 - Financial transactions
- Logs are:
 - Stored securely
 - Reviewed regularly

INCIDENT RESPONSE POLICY

Definition

An incident includes:

- Data breaches
- Unauthorised access
- System compromise
- Fraud or suspicious activity

All incidents must be recorded in the **Incident Log (Appendix B)**.

Incident Classification

- **Low** – No sensitive data affected
- **Medium** – Limited operational or data impact
- **High / Critical** – Player data, funds, or systems compromised

Incident Response Process

1. **Identify** – Detect and log the incident
2. **Contain** – Prevent further impact
3. **Investigate** – Determine root cause
4. **Remediate** – Fix vulnerabilities
5. **Recover** – Restore systems
6. **Document** – Record actions taken

Regulatory Reporting

Where required, the Company will notify:

- **Curaçao Gaming Authority (CGA)**
- Relevant data protection authorities

Within applicable timeframes (typically **within 72 hours** for material incidents)

Communication

- Affected users will be notified where appropriate
- Internal stakeholders will be informed promptly

THIRD PARTY & VENDOR DUE DILIGENCE FRAMEWORK

Applies to:

- Payment Service Providers (PSPs)
- Game providers
- Platform providers
- IT and infrastructure vendors

Due Diligence (Pre-Onboarding)

The Company assesses:

- Regulatory status and licensing
- Reputation and track record
- Security practices
- Data handling procedures

Contractual Requirements

All vendors must:

- Comply with data protection laws
- Maintain appropriate security controls
- Notify the Company of any incidents affecting Company data

Access Controls

- Vendor access must be:
 - Approved
 - Time-limited

- Monitored

Ongoing Monitoring

- Vendor risk is reviewed periodically
- High-risk vendors are subject to enhanced oversight

BACKUP & BUSINESS CONTINUITY

- Data is backed up at least daily
- Backups are:
 - Encrypted
 - Stored in secure, geographically separate locations
 - Regularly tested

The Company maintains:

- Disaster Recovery procedures
- Business Continuity arrangements

DEVICE & REMOTE WORKING SECURITY

- Only secure devices may access Company systems
- Devices must:
 - Be password protected
 - Be regularly updated
- Lost or stolen devices must be reported immediately

TRAINING & AWARENESS

- Staff receive:
 - Security training at onboarding
 - Ongoing awareness training
- Includes:
 - Phishing awareness
 - Data protection responsibilities

COMPLIANCE & REVIEW

- This policy is reviewed:

- At least annually
 - Upon significant changes
- Compliance is monitored by the KCF

CONTINUOUS IMPROVEMENT

The Company is committed to:

- Continuous improvement of its Information Security Framework
- Adapting controls to:
 - Emerging threats
 - Regulatory developments
 - Business changes

APPENDIX A – INFORMATION SECURITY RISK REGISTER

Risk Description	Category	Likelihood	Impact	Risk Rating	Controls in Place	Mitigation Actions	Owner
PSP failure, delays, or fraudulent transactions impacting player funds	Financial / Payments	3	5	15	Use of established PSPs, transaction monitoring	Diversify PSPs, enhance transaction monitoring rules	Operations
Failure or breach of third-party platform	Third Party	2	5	10	Reliance on platform provider controls, contractual arrangements	Increase oversight, security assurances, contingency plan	KCF
Platform downtime or infrastructure outage	Availability	3	3	9	Hosting redundancy, provider SLAs	Define DR expectations with providers, monitor uptime	IT
Internal error leading to data exposure (e.g. human error)	Internal	3	3	9	Limited access, role-based permissions	Improve change controls and internal review processes	KCF
Delayed or failure to report a notifiable incident to CGA	Regulatory	1	5	5	Incident response process defined	Formalise escalation triggers and responsibilities	KCF
Unauthorised privileged access to back-office systems	Access Control	1	5	5	RBAC, limited admin users, MFA	Periodic access reviews, stricter privilege separation	IT
Compromise of player accounts via credential stuffing/phishing	Data Security	1	5	5	MFA, hashed passwords, login monitoring	Introduce forced MFA, improve login anomaly detection	IT

Scoring Methodology:

- Likelihood: 1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost Certain
- Impact: 1 = Minimal, 3 = Moderate, 5 = Severe (financial, regulatory, or reputational impact)
- Risk Rating = Likelihood × Impact

APPENDIX B – INCIDENT LOG & REGISTER

Incident ID	Date	Description	Severity	Systems Affected	Action Taken	Status	Reported to CGA	Owner
INC-001	07-Jan-26	Suspicious login attempt detected	Low	Player accounts	Forced password reset	Closed	No	IT
INC-002	22-Feb-26	Temporary platform downtime	Medium	Website	Restarted services, issue resolved	Closed	No	IT