
Information Security Policy

Owner	Author	Board Approval	Review Date	Next review date	Version	Comment
Compliance Officer	LNS	19/04/2026	19/04/2026	19/04/2027	V1.0	New Document

Contents

1. Purpose & Scope.....3

2. Regulatory and Legal Basis3

3. Information Security Objectives4

4. Governance and Responsibilities4

5. Internal Information Security Standards4

6. External Threat Protection6

7. Incident Response and Reporting.....7

8. Infrastructure, Network and System Security7

8. Gaming System Integrity and Player Protection.....7

9. REVIEW AND MONITORING7

1. Purpose & Scope

1.1. The purpose of this Information Security Policy (“the Policy”) is to establish the framework by which Dynamik Marketing (“The Company”) protects its information assets, gaming systems, player data, financial records and operational infrastructure.

1.2. This Policy is intended to safeguard the confidentiality, integrity and availability of all systems and data associated with the Company’s licensed e-gaming operations and to ensure the Company operates safely, responsibly, transparently and reliably in accordance with Curacao licensing requirements.

1.3. This Policy further establishes the minimum standards and expected behaviours for employees, contractors, vendors and third parties to mitigate both internal and external security threats, including but not limited to phishing, fraud, hacking, unauthorised disclosure of sensitive information, misuse of customer data and operational disruption.

1.2. This policy applies to:

- All employees, directors, key persons, contractors and third-party vendors who access Company Information systems or process player or financial data
- All information systems, gaming equipment, servers, networks, endpoints, and cloud services owned, leased, or operated by the Company
- All player data, financial transactions data, gaming transactions data, and any other data held or processed in connection with licensed operations.
- All company domains and sub-domains approved under the CGA license.

2. Regulatory and Legal Basis

2.1. This Policy is designed to comply with all the legal and regulatory requirements including LOK, CGA Online gaming conditions, the CGA Technical requirements, National Ordinance on Identification in Service Provision, and any applicable data protection principles consistent with international standards, even if adopted as best practice.

2.2. The Company may implement additional controls where necessary to meet evolving regulatory expectations or operational risk.

3. Information Security Objectives

3.1. Dynamik Marketing commits to:

- Confidentiality – ensuring that player and business information is accessible only to authorised persons.
- Integrity – safeguarding the accuracy and completeness of information and gaming systems
- Availability – ensuring that gaming systems, player accounts and critical data remain accessible in accordance with operational and regulatory requirements.
- Accountability – maintaining audit trails that allow the CGA and authorised parties to verify compliance at all times.

4. Governance and Responsibilities

4.1. Board of Directors have the ultimate accountability for information security and ensuring adequate resources are allocated to Information Security.

4.2. CTO has day-to-day ownership and implementation of this policy ensuring annual review of this policy to ensure it is still up to date and aligned to requirements.

4.3. The Compliance Officer will monitor compliance with the LOK license conditions, including this Policy and will liaise with the CGA on regulatory matters.

4.4. All staff must ensure adherence to this policy and related procedures at all times and report any security incident, vulnerabilities or suspected breaches identified without delay.

5. Internal Information Security Standards

5.1. Acceptable Use. Company systems, devices and network resources must be used only for authorised business purposes. Limited personal use may be permitted where it:

- Does not interfere with business operations;
- Does not violate applicable laws or Company policies; and
- Does not introduce security risks to Company systems.

Users must not:

- Attempt to bypass security controls
- Access unauthorised systems or data
- Install unapproved software; or
- Use Company systems for unlawful, offensive or malicious purposes

5.2. Password management. Strong and unique passwords must be used for all Company systems and accounts. The following minimum requirements apply:

- Passwords must not be shared or reused across systems

- Multi-factor authentication (“MFA”) must be enabled for remote access, administrative access and critical systems
- Passwords and authentication credentials must be stored securely using approved methods
- Default credentials must be changed immediately upon deployment of systems or applications

5.3. Access Control. Access to systems, application, and data is granted on a privilege and need to know basis. User access request must be approved by authorised management and reviewed periodically.

The Company shall ensure that:

- User access is formally approved by authorised personnel
- Access rights are reviewed periodically
- Privileged access is restricted and monitored
- Access is revoked promptly following termination, suspension or role changes
- Shared accounts are prohibited unless formally approved and monitored

5.4. Data Classification and Handling. Information assets must be classified according to sensitivity and business criticality. Data classifications may include:

- Public
- Internal
- Confidential
- Restricted

Confidential and restricted data, including player information, authentication credentials, financial records and gaming transaction data, must be:

- Encrypted at rest and in transit
- Access-controlled
- Retained and disposed of securely in accordance with legal and operational requirements

5.5. Device and Endpoint Security. All Company-managed devices must:

- Use approved antivirus and endpoint protection solutions
- Be configured according to Company security standards
- Receive regular security updates and patching
- Be protected with password/PIN or biometric authentication
- Be locked when unattended.

The use of personal devices to access Company systems may only occur where formally approved and subject to security controls.

5.6. Security awareness and training. Staff must complete mandatory information security and compliance training upon onboarding and regularly thereafter. The Company may conduct phishing

simulations, awareness campaigns, refresher training and targeted training for privileged or high-risk roles. Staff are required to immediately report suspected phishing attempts, fraud, vulnerabilities or security incidents.

6. External Threat Protection

6.1. Phishing and Social Engineering. The company shall implement measures to identify and mitigate phishing, impersonation and social engineering threats. These measures may include:

- Email filtering and monitoring
- Domain protection controls
- Security awareness campaigns
- Monitoring for suspicious communications and account activity.

Players and customer may also be provided with guidance on recognising phishing attempts and protecting their accounts.

6.1. The Company shall maintain controls designed to detect suspicious gaming activity, payment fraud, accounts abuse and potential AML/CTF risks. Such controls may include:

- Automated fraud monitoring systems
- Transaction monitoring
- Behavioural analytics
- Geolocation and device intelligence
- Risk based customer verification measures
- Escalation procedures for suspicious activity

6.3. Protection against hacking and cyber threats. The Company shall implement layered technical and organisational security controls, including firewalls, intrusion detection and prevention systems, Web application firewalls, Network segmentation, continuous monitoring and vulnerability management processed. Regular vulnerability assessments and penetration testing shall be conducted by qualified personnel or independent third parties where required.

6.4. Secure Software development. Gaming systems, internal tools and software applications must be developed and maintained using secure development practices. This includes security testing prior to deployment, code reviews, vulnerability scanning, secure configuration management, change management procedures and assessment of third party libraries and dependencies. The Company may operate internal vulnerability reporting or responsible disclosure processes to identify and remediate security weaknesses.

6.5. Software installation and change control. Software downloads and installations on Company systems are restricted. No software, applications or executables may be installed without prior approval from authorised IT staff. All production changes must follow approved change management and testing procedures before implementation.

7. Incident Response and Reporting

7.1. All personnel must immediately report security incidents, suspected data breaches, system vulnerabilities, unauthorised access attempts or suspicious activities.

7.2. The Company will maintain an incident response framework designed to identify and assess incidents, contain threats, investigate root causes, remediate vulnerabilities, restore affected systems and meet applicable regulatory notification obligations.

7.3. Where required by law or regulatory conditions, affected parties and competent authorities shall be notified within applicable timeframes.

8. Infrastructure, Network and System Security

8.1. Critical gaming and operational systems shall be hosted within secure environments appropriate for licensed e-gaming operations.

8.2. The Company will maintain secure hosting infrastructure, segregated environments for production, testing and development, backup and disaster recovery capabilities, redundancy and resilience controls, continuous system monitoring.

8.3. Data transmitted over public or untrusted networks must be encrypted using industry-standard encryption protocols.

8. Gaming System Integrity and Player Protection

8.1. Gaming systems, including Random Number Generators are tested and certified in accordance with applicable CGA and recognised industry standards.

8.2. Gaming software is subject to security, fairness, and integrity measures and the Company will ensure it'll maintain auditability of gaming operations and accurate recording of gaming activity.

9. REVIEW AND MONITORING

9.1. This policy is a living document designed to evolve alongside the business operations, regulatory environment and risk profile. While the fundamental principles will remain constant, periodic reviews

are required to ensure alignment with legislation, regulation, business processes and risk appetite. This policy will be formally reviewed at least annually, or earlier if material changes occur in applicable regulations, internal controls or identified risks.

9.2. Any updates or amendments will be documented, version controlled and communicated promptly to all relevant staff.

9.3. The latest approved version of this policy is available to all staff via the company's SharePoint site and it is the responsibility of each staff member to familiarise themselves with the most current version.

9.4. Evidence of review and Board approval (where required) will be retained to support ongoing oversight and demonstrate compliance with governance requirements.