1, Abraham de Veerstraat, Curaçao **15/09/2025**

Information Security Policy

NEXUS INTERNATIONAL ENTERTAINMENT N.V.

---

by: **Morganite Corporate Services B.V.**

Director of: **NEXUS INTERNATIONAL ENTERTAINMENT N.V.**

Purpose

We at **NEXUS INTERNATIONAL ENTERTAINMENT N.V.** licensed by the Curaçao Gaming Authority (License No. OGL/2024/1324/0750), are responsible for operating the gaming platform luckypari.com. In doing so, we manage highly sensitive information, including customer records, payment data, and business documentation.

This policy sets out the principles, responsibilities, and controls we adopt to ensure the confidentiality, integrity, and availability of all information under our care. It also demonstrates our commitment to regulatory compliance and international security standards.

Scope

This policy applies to all individuals and organizations working with or on behalf of the Company, including employees, contractors, consultants, and service providers.

It covers:

- All systems and infrastructure, including servers, networks, applications, and backup environments.
- All categories of data, from customer and financial information to regulatory filings and operational records.
- All third parties and partners who support our services.

Our Security Principles

Our approach to security is guided by the following values:

1. **Confidentiality** – Sensitive data is protected against unauthorized access or disclosure.
2. **Integrity** – Information is maintained in an accurate, reliable, and trustworthy state.
3. **Availability** – Services and data remain accessible when required, supported by backup and recovery capabilities.
4. **Accountability** – Every individual has a defined responsibility in safeguarding information.
5. **Compliance** – Our practices align with applicable laws, licensing conditions, and recognized international standards.

Security Measures

- **Infrastructure Protection** – We maintain layered defenses, including firewalls, intrusion prevention systems, DDoS mitigation, and encrypted communication channels.
- **Access Control** – We apply the principle of least privilege, reinforced through strong authentication, regular reviews, and immediate revocation of access when roles change.
- **Data Security** – Data at rest and in transit is encrypted. Where possible, sensitive identifiers are masked or pseudonymized.
- **Applications and Endpoints** – We follow secure coding standards, conduct penetration testing, and implement company-approved device protections.
- **Monitoring and Auditing** – Security activity is continuously monitored, logged, and reviewed. Independent audits confirm the effectiveness of our controls.
- **Third-Party Oversight** – Suppliers are vetted before engagement and contractually required to meet our security standards. Compliance is reviewed periodically.

Responsibilities of Staff

All staff and contractors share responsibility for protecting information. This includes:

- Completing mandatory training on cybersecurity, anti-fraud, and regulatory compliance.
- Reporting incidents or vulnerabilities without delay.
- Using only authorized, company-managed devices and software.
- Undergoing background checks where responsibilities involve sensitive access.

Incident Management

We maintain a structured incident response plan to ensure that breaches or suspected breaches are identified, contained, and investigated promptly.

We commit to:

- Notifying regulators, affected individuals, and partners transparently and within legal timeframes.
- Implementing recovery measures to restore operations.

- Capturing lessons learned and updating procedures accordingly.

Risk Management

We evaluate and monitor information security risks on a regular basis. This includes:

- Formal risk assessments and annual reviews.
- Maintaining a central register of risks, ranked by likelihood and impact.
- Addressing emerging threats, including cybercrime, fraud, and gaming abuse.

Compliance

Compliance with this policy is mandatory.

- Employees who fail to comply may face disciplinary action.
- Partners who breach security obligations may face termination of contracts and regulatory reporting.
- Maintaining compliance with this policy is considered a fundamental condition of employment and partnership.

Continuous Improvement

This policy is reviewed at least annually or sooner if required by regulatory changes, new technologies, or significant security events. Updates are recorded and communicated across the Company.

We remain committed to investing in tools, processes, and training to strengthen our defenses and sustain the trust of our stakeholders.

Governance

The Board of Directors holds ultimate responsibility for information security.
Day-to-day management is delegated to the Chief Technology Officer (CTO), who ensures appropriate resources and oversight.

Independent audits provide assurance to regulators, partners, and customers that we operate securely, responsibly, and with integrity.