

Information Security Policy

Purpose

This Information Security Policy establishes the principles, responsibilities, and practices by which Spinzz.com protects its information assets, systems, and users. The Company acknowledges that its operations involve the collection and processing of highly sensitive data, including player identification records, payment transactions, gaming history, and internal operational documents. The purpose of this policy is to provide a structured framework for ensuring the confidentiality, integrity, and availability of all such data and systems, while meeting the requirements of the Curaçao National Ordinance on Games of Chance (LOK), directives of the Curaçao Gaming Authority (CGA), and other applicable laws and standards. This Policy also demonstrates the Company's ongoing commitment to risk management, customer trust, and operational resilience, ensuring that Spinzz.com remains a safe, transparent, verifiable, and reliable licensed operator.

1. Statement

Spinzz.com is firmly committed to protecting the confidentiality, integrity, and availability of all systems and data under its control. The Company recognizes that information security is essential to the protection of its customers, staff, and overall business operations.

Unauthorized access, misuse, or loss of data can undermine trust, expose the Company to legal liabilities, and disrupt gaming services. Therefore, Spinzz.com maintains an information security management framework that ensures threats are identified, controls are applied, and risks are minimized to an acceptable level. The Company's management actively supports and oversees the implementation of this policy and provides the resources necessary to uphold it.

2. Scope

This Policy applies across the entire environment in which Spinzz.com operates. It covers the gambling platform and all supporting business systems, including financial gateways, KYC/AML systems, risk monitoring tools, affiliate platforms, and customer relationship management solutions. It applies to all employees of Spinzz.com, contractors engaged in operational support, and any authorized third parties who have access to Company systems or data.

The Policy extends to all devices, whether owned by the Company or used remotely under secure conditions, and to all methods of data storage, whether located on-site, in the cloud, or through third-party service providers. Compliance with this Policy is a condition of employment, contract engagement, and vendor partnership.

3. Principles

Spinzz.com adheres to several fundamental principles of information security. All

information is classified according to sensitivity, with categories including:

Restricted

- Player KYC documentation (passports, IDs, proof of address, bank statements)
- Payment card details and bank account information
- System administrator credentials, API keys, encryption keys
- AML/CTF investigation files, SAR/UTR reports
- Detailed incident reports and forensic data

Confidential

- Internal compliance manuals and security policies
- Employee HR records and contracts
- Risk management assessments and audit findings
- Detailed financial reports not for public disclosure
- Internal fraud monitoring or suspicious player activity logs

Internal

- General staff communications and notices
- Operational procedures (non-sensitive SOPs)
- Internal meeting notes and progress reports
- Training materials for employees
- Non-sensitive performance metrics or dashboards

Public

- Spinzz.com website content and promotional material
- Public announcements and press releases
- Terms & Conditions, Responsible Gaming policy, and Privacy Policy published on the site
- Marketing campaigns and affiliate resources
- Job postings and publicly shared company information

Access to systems and data is granted strictly on a need-to-know basis, with privileges aligned to defined roles and withdrawn immediately once no longer required.

Information is protected from unauthorized access, loss, corruption, or misuse through technical safeguards such as encryption, firewalls, and monitoring tools, as well as through organizational measures such as staff training and segregation of duties.

The Company ensures that its systems are continuously updated with security patches, monitored for unusual or suspicious behavior, and regularly backed up to prevent data loss. Any incidents, breaches, or near-misses are reported promptly, logged in a secure register, investigated by the Information Security Officer, and addressed with corrective action.

4. Legal & Regulatory Compliance

Spinzz.com ensures that its practices are aligned with all relevant data protection and gambling regulatory obligations. The Company complies with the Curaçao LOK and the requirements issued by the CGA, including obligations to maintain safe, transparent, verifiable, and reliable systems. It adheres to the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NORUT) and the National Ordinance on the Supervision of Online Games of Chance (NOIS), ensuring proper retention of customer data for AML/CTF purposes and timely reporting of unusual or suspicious transactions.

Spinzz.com also observes the National Ordinance on Personal Data Protection and, where applicable, the General Data Protection Regulation (GDPR), to ensure that personal information is collected and processed lawfully, fairly, and securely. The Company benchmarks its practices against ISO/IEC 27001 principles and other industry best practices, providing assurance to regulators, players, and partners that information security is managed in a structured, auditable, and internationally recognized manner.

5. Key Controls (Framework)

Spinzz.com has established a framework of key controls to mitigate risks and uphold information security. Risk management processes are in place to ensure regular assessment of threats and vulnerabilities. Risks are documented in a formal register, evaluated for likelihood and impact, and addressed with treatment measures such as mitigation, transfer, or acceptance, under the oversight of senior management.

Access control procedures ensure that user accounts are managed responsibly, with clear approval processes for granting access and strict rules for revoking access when an employee or contractor leaves. Remote access is permitted only through secure VPN connections combined with multi-factor authentication. Segregation of duties is applied to prevent conflicts of interest, particularly in areas such as payments and withdrawals.

Personal devices may only be used with prior approval by a Company Director and are limited to email and calendar functions under secure, encrypted containers. Company equipment is safeguarded through the use of firewalls, antivirus solutions, encryption of data, and strong password policies.

The Company enforces strict email security practices. Employees are prohibited from unlawful use of Company email, and suspicious messages must be reported immediately.

All confidential data is encrypted both in storage and during transmission, and backup procedures are applied daily. Backups are encrypted, stored in secure geographic locations, and tested regularly to ensure their integrity and effectiveness.

6. Incident Handling

Spinzz.com maintains a clear incident response framework to ensure that security events are handled quickly and effectively. All staff are obligated to report any suspected or actual security incident to the Information Security Officer without delay.

Each incident is logged in an official register, categorized according to severity, and investigated thoroughly to determine its cause and impact. Corrective and preventive actions are applied to contain and resolve the incident.

Where legally required, incidents are reported to the Curaçao Gaming Authority and the Data Protection Authority within seventy-two hours. After each incident, a review is conducted to ensure lessons are learned and controls are updated to reduce the likelihood of recurrence.

7. Review

This Policy is reviewed at least once every twelve months, or earlier if significant changes occur in systems, processes, or regulatory requirements. The review process involves a full evaluation of the Policy's effectiveness, including whether it continues to meet legal obligations, addresses current risks, and aligns with evolving best practices.

Any updates to the Policy must be formally approved by the Board of Directors, and employees are informed of changes to ensure continued compliance.

8. Contacts

Director (Information Security responsible): Mr. Boy Hendriks, cs@softgamings.com