

Information Security Policy Rolsbet

For <https://www.rolsbet.com> NUMERETO B.V.

01.09.2025

Approved by Board of Directors

Introduction and Purpose

NUMERETO B.V., operating <https://www.rolsbet.com>, conducts online gaming operations that require the continuous protection of sensitive information. The Company acknowledges that personal data, financial details, gaming records, and business documentation are valuable assets requiring the highest level of safeguarding.

The purpose of this Policy is to provide a coherent and consistent framework for securing all such assets. The objectives are to ensure confidentiality, integrity, availability, and resilience of information, while supporting the Company's ability to provide secure, fair, and transparent gaming services. This Policy also demonstrates the Company's commitment to compliance with Curaçao regulations, international data protection standards, anti-money laundering rules, and recognized industry best practices.

Scope

This Policy applies to all individuals working for or with NUMERETO B.V., including employees, contractors, advisors, consultants, and external suppliers. It governs all IT systems, applications, infrastructure, and related services, including data centers, disaster recovery sites, and cloud-based platforms.

The Policy applies to all data processed by the Company, including player accounts, payment information, operational records, regulatory submissions, and monitoring logs. It also extends to third-party service providers delivering essential support, who must adhere to equivalent security standards.

Guiding Principles

- **Confidentiality:** Access to sensitive data is restricted and governed by strict access controls, strong authentication, and robust encryption mechanisms.
- **Integrity:** Information must remain accurate and complete. Systems are monitored for unauthorized modifications and are subject to validation and independent reviews.
- **Availability:** Services must remain consistently available to authorized users. Business continuity plans, redundancy, and failover measures ensure resilience.

- **Accountability:** Responsibilities are clearly defined. Each individual handling data is personally accountable for maintaining its security.
- **Compliance:** All security measures comply with local and international regulations, including ISO/IEC 27001 standards, GDPR principles, AML/CTF obligations, and gaming sector rules.
- **Transparency:** Policies and procedures are documented and communicated to all relevant stakeholders, ensuring clarity of responsibilities.

Security Framework

Network and Infrastructure Defense

The Company implements layered security, including firewalls, VPN access, anti-malware systems, DDoS mitigation, and real-time monitoring. All connections (gaming, payments, and internal administration) are encrypted using current best-practice protocols.

Identity and Access Management

Access rights are granted on a role-based, least-privilege basis. Multi-factor authentication is required for all privileged accounts. Permissions are reviewed quarterly, and revoked immediately upon employee departure or contract termination.

Data Protection

Data is encrypted both at rest and in transit. Sensitive records may be tokenized or anonymized to further mitigate risk. Regular testing ensures compliance with data protection requirements.

Application and Endpoint Security

All applications are developed under secure coding practices. Independent penetration testing and vulnerability scans are conducted quarterly. Employee devices are controlled by endpoint management, ensuring compliance with corporate security baselines.

Cloud Security

Where cloud-based systems are used, providers must demonstrate compliance with international certifications such as ISO/IEC 27017 and SOC 2 Type II. Contracts impose obligations regarding data handling and breach notification.

Monitoring, Logging, and Audit

All security events are logged, analyzed, and stored in tamper-proof environments. Monitoring tools identify anomalies in real time. Independent internal and external audits validate compliance with obligations.

Supplier Risk Management

Critical suppliers must undergo due diligence and periodic reviews. Contractual

obligations require them to maintain equivalent levels of information security and notify the Company of any incidents.

Employee Responsibilities

Employees and contractors must complete annual security training covering data protection, cybersecurity awareness, AML/CTF, and incident response. They are required to report security concerns immediately. Failure to comply may result in disciplinary or legal action.

Background checks are mandatory for employees in sensitive roles. Only authorized hardware, managed through corporate IT, may be used for company operations.

Incident Response and Breach Management

The Company maintains a tested incident response framework to ensure:

1. Prompt identification, escalation, and containment of incidents.
2. Thorough investigation into cause, scope, and impact.
3. Mandatory notifications to regulators, customers, and stakeholders in compliance with law.
4. Timely restoration of affected systems and services.
5. Post-incident reviews, with findings integrated into future controls.

Risk Management

Risks are assessed continually, with formal reviews at least once per year and whenever new technology or business processes are introduced. Independent experts conduct penetration tests, audits, and gaming software reviews.

All risks are logged in a central register, ranked by likelihood and severity, and mitigated through technical, administrative, and organizational measures.

Business Continuity and Disaster Recovery

The Company maintains a business continuity plan and disaster recovery strategy to ensure minimal disruption in the event of operational or technological failure. This includes:

- Backup and replication of critical systems.
- Testing of recovery procedures at least twice per year.
- Clear escalation paths and communication strategies in crisis situations.

Compliance and Enforcement

This Policy is mandatory. Non-compliance by employees may lead to disciplinary measures up to termination of employment. Supplier non-compliance may result in contract termination or reporting to regulators.

Compliance with this Policy is a condition of employment, engagement, and partnership. The Company acknowledges that its licensing obligations require strict adherence to secure and responsible business practices.

Review and Continuous Improvement

This Policy is reviewed at least annually, and earlier where regulatory, technological, or business developments necessitate change. Updated versions are approved by senior management and communicated across the organization.

Information security is an evolving practice. NUMERETO B.V. invests in emerging technologies, adopts improved practices, and promotes security awareness as part of its corporate culture.

Governance

The Board of Directors retains ultimate responsibility for the Company's information security. Oversight of implementation and enforcement rests with the Chief Information Security Officer (CISO). Adequate resources, staff, and controls are ensured.

External and internal audits provide assurance of compliance, offering confidence to regulators, partners, and players that NUMERETO B.V. operates at the highest level of integrity and security.

Approved by **Olena Chuchman** Director of NUMERETO B.V.

