

INFORMATION SECURITY POLICY

For ORAKUM N.V.

Effective Date: September 16, 2025

Approved by: Board of Directors

1. INTRODUCTION AND PURPOSE

ORAKUM N.V. conducts licensed online gaming activities which depend upon the secure and uninterrupted processing of sensitive information. The Company recognizes that personal data, financial records, gaming transactions, and operational documents are strategic assets requiring the highest level of protection.

The purpose of this Information Security Policy is to establish a comprehensive governance framework ensuring the confidentiality, integrity, and availability of information assets, while safeguarding the Company's operational resilience and reputation. By adopting this Policy, ORAKUM N.V. affirms its commitment to compliance with applicable data protection laws, anti-money laundering obligations, and gaming-sector regulations, as well as to alignment with internationally recognized standards such as ISO/IEC 27001.

2. SCOPE

This Policy applies to all employees, officers, contractors, consultants, and third-party service providers engaged by ORAKUM N.V. It governs all systems, applications, servers, and related infrastructure deployed in the provision of gaming services, including data centers, backup environments, and disaster recovery solutions.

The Policy covers all information processed by ORAKUM N.V., regardless of its format or medium, and extends to suppliers and business partners whose services support the Company's operations.

3. GUIDING PRINCIPLES

ORAKUM N.V. upholds the following core principles as the foundation of its information security management:

- 1) **Confidentiality:** All sensitive and proprietary information must be shielded from unauthorized disclosure or misuse. Access privileges are

strictly determined by role-specific necessity and reinforced by encryption, secure authentication, and controlled dissemination of data.

- 2) **Availability:** Critical systems and information resources must be reliably accessible to duly authorized users whenever required. Business continuity is preserved through redundancy, secure backups, and tested disaster recovery arrangements that guarantee minimal disruption.
- 3) **Accountability:** Clear lines of responsibility for information protection are established at every level of the organization. Each employee, contractor, or partner entrusted with data is obligated to act with diligence and is personally answerable for maintaining security standards.
- 4) **Integrity:** The Company ensures that information remains accurate, reliable, and uncorrupted throughout its lifecycle. Systems and processes are built with safeguards to prevent unauthorized alterations, supported by continuous monitoring, validation checks, and independent assurance reviews.
- 5) **Compliance:** Security practices are aligned with both local Curaçao regulatory requirements and international legal frameworks, while reflecting global standards and sector-specific benchmarks such as ISO/IEC 27001. ORAKUM N.V. continuously adapts to evolving regulatory obligations and industry best practices to ensure lawful and responsible operations.

4. SECURITY FRAMEWORK

- 1) **Network and Infrastructure Protection.** The Company implements a defense-in-depth model to protect its technological environment. This includes the deployment of enterprise-grade firewalls, intrusion detection and prevention systems (IDPS), DDoS mitigation tools, and secure VPN connections. All communications — including gaming interactions and financial transactions — are encrypted using current industry standards (TLS/SSL). Infrastructure components are subject to continuous hardening, patching, and configuration management.
- 2) **Identity and Access Management.** Access to corporate systems and sensitive information is strictly controlled under the principle of “least privilege.” Each user is granted only those permissions required to perform assigned functions. Multi-factor authentication, session timeouts, and privileged access monitoring are mandatory. User access rights undergo

quarterly reviews, and entitlements are immediately revoked upon termination or role change.

- 3) **Data Security and Protection.** All personal and financial data are encrypted at rest and in transit using strong cryptographic standards. Key management procedures ensure that encryption keys remain secure and traceable. Wherever feasible, identifiers and sensitive attributes are anonymized or pseudonymized to mitigate re-identification risk. Data retention and deletion practices comply with applicable data protection legislation.
- 4) **Application and Endpoint Protection.** ORAKUM N.V. follows secure development lifecycle (SDLC) principles to safeguard its gaming and operational platforms. Regular code reviews, penetration testing, vulnerability assessments, and third-party certifications validate system integrity. All company-managed endpoints, including employee laptops and mobile devices, are secured by mobile device management (MDM) and endpoint detection and response (EDR) solutions. Unauthorized applications and removable media are prohibited.
- 5) **Monitoring, Logging, and Audit Controls.** The Company operates centralized monitoring through Security Information and Event Management (SIEM) solutions. Security logs are collected, preserved in secure high-availability storage, and analyzed in real time to detect anomalies. Internal audit reviews are carried out on a periodic basis, supplemented by independent external audits to verify compliance with regulatory and internal requirements.
- 6) **Third-Party and Supplier Security.** Vendors, contractors, and service providers who have access to critical systems or sensitive data must adhere to ORAKUM N.V.'s security standards. Formal due diligence and risk assessments are conducted prior to engagement. Contracts impose mandatory obligations relating to data protection, incident reporting, and compliance monitoring. Periodic reassessments and audits validate that third-party partners continue to meet the Company's requirements.

5. EMPLOYEE RESPONSIBILITIES

Information security is a collective duty shared by every individual engaged with ORAKUM N.V., regardless of their role or seniority. To maintain a secure environment, the following obligations apply:

5.1. Training and Awareness

- All employees, contractors, and consultants must complete mandatory induction training on cybersecurity, data protection, and anti-money laundering/counter-terrorist financing (AML/CTF) requirements.
- Refresher training sessions are conducted at least annually, supplemented by targeted awareness campaigns addressing emerging risks (e.g., phishing, social engineering, ransomware).
- Records of participation in training are maintained as evidence of compliance.

5.2. Incident and Risk Reporting

- Every staff member is required to immediately report any actual or suspected security incident, vulnerability, or system weakness through designated reporting channels.
- Reports must be made without delay and without fear of retaliation; failure to report may constitute a disciplinary breach.
- A “see something, say something” culture is actively encouraged to ensure proactive threat detection.

5.3. Pre-Employment Screening

- Personnel whose duties involve access to sensitive data, financial information, or system administration undergo enhanced background verification.
- Screening may include checks of professional integrity, criminal records (where legally permissible), financial soundness, and references.
- Employment offers for critical roles remain conditional upon the successful completion of such checks.

5.4. Acceptable Use of Technology

- Only company-approved devices, applications, and communication tools may be used to access ORAKUM N.V.’s internal systems.
- The installation or use of unauthorized hardware, software, or storage media is strictly prohibited.
- Employees must comply with “clean desk” and “screen lock” requirements to prevent inadvertent disclosure of sensitive information.

5.5. Accountability and Disciplinary Measures

- Each individual is personally responsible for safeguarding credentials, devices, and data entrusted to them.
- Misuse of systems, negligence in handling data, or breach of security obligations may result in disciplinary action, up to and including termination of employment or contract.
- In cases involving deliberate misconduct or gross negligence, ORAKUM N.V. reserves the right to pursue legal remedies.

6. INCIDENT RESPONSE AND BREACH MANAGEMENT

The Company maintains a formal incident response plan to address any event that could compromise information security. The plan ensures that:

ORAKUM N.V. maintains a formal Incident Response Plan to ensure that any security incident is managed swiftly and effectively. The Plan provides that:

- Identification and Containment: Incidents are promptly detected and isolated to minimize impact.
- Investigation: Root causes and consequences are assessed and documented.
- Notification: Regulators, affected customers, and stakeholders are informed in line with legal requirements.
- Recovery: Systems and services are restored to normal operation without undue delay.
- Improvement: Lessons learned are incorporated into updated procedures to prevent recurrence.

7. RISK MANAGEMENT

Information security risks are assessed on an ongoing basis. Comprehensive reviews are conducted annually and whenever significant changes occur in technology or operations. Independent penetration testing, system audits, and gaming software certifications form part of the risk management process.

Identified risks are recorded in a structured register, prioritized according to impact and likelihood, and mitigated through appropriate technical and organizational measures. The risk management process also considers emerging threats, including fraud, cybercrime, and misuse of gaming systems.

8. COMPLIANCE AND ENFORCEMENT

This Policy is mandatory. Employees who violate its provisions may face disciplinary measures up to and including dismissal. Breaches by suppliers or

partners may result in termination of agreements and, where required, reporting to regulatory authorities.

ORAKUM N.V. recognizes that its gaming license depends upon secure, transparent, and responsible operations. It therefore treats compliance with this Policy as a condition of employment, partnership, and continued operation.

9. REVIEW AND CONTINUOUS IMPROVEMENT

This Policy is reviewed at least once a year, or more frequently if regulatory requirements change, if major technological changes occur, or if significant incidents reveal areas for improvement. Updates are documented, approved by senior management, and communicated to all employees and partners.

Information security is not a static requirement but a process of continuous improvement. By investing in new technologies, adapting to evolving threats, and fostering a culture of awareness, the Company ensures that its security posture remains strong and that its operations remain worthy of trust.

10. GOVERNANCE

The Board of Directors of ORAKUM N.V. holds ultimate responsibility for information security and is accountable for ensuring that the Company's operations remain secure, transparent, and compliant. The Board ensures that adequate resources, procedures, and controls are established and maintained to safeguard the Company's information assets.

Independent internal reviews and external audits are carried out on a regular basis to confirm compliance with regulatory requirements, to verify the effectiveness of security measures, and to provide assurance to regulators, business partners, and players that ORAKUM N.V. operates with integrity and the highest standards of security.

Approved and signed by Serhii Yelovatskyi



Director of ORAKUM N.V.