

Information Security Policy

For <https://vippari.com> Geosix B.V.

Effective Date: 01.09.2025

Approved by: Board of Directors

Overview and Intent

<https://vippari.com>, managed by Geosix B.V., delivers online gaming services that necessitate the secure and uninterrupted processing of confidential data. The Company acknowledges that personal information, financial details, gaming activities, and business records are critical assets requiring stringent protection.

This Information Security Policy establishes a comprehensive structure to safeguard these assets. Its goal is to uphold the confidentiality, integrity, and accessibility of data while ensuring the Company can offer gaming services in a secure, open, and ethical manner. Through this Policy, the Company commits to fulfilling all relevant data privacy, anti-money laundering, and gaming industry regulations, while adhering to widely accepted global security benchmarks.

Applicability

This Policy extends to all individuals affiliated with the Company, encompassing employees, contractors, consultants, and external vendors. It regulates all technological platforms, software, servers, and networks employed in gaming operations, as well as supporting infrastructure such as data storage facilities, backup systems, and disaster recovery protocols. The Policy encompasses all data handled by the Company, irrespective of its form, including player profiles, monetary transactions, corporate files, system records, and compliance-related reports. It also applies to suppliers providing vital support to the gaming platform, mandating that they uphold comparable security standards.

Core Principles

The Company's approach to information security is shaped by the following foundational principles:

- **Confidentiality:** Confidential information must be shielded from unauthorized viewing or sharing. Access is granted only as needed for business purposes, reinforced by advanced authentication and encryption techniques.
- **Integrity:** Data must remain accurate, unaltered, and dependable. Systems are built to identify and thwart modifications, supported by regular independent assessments.
- **Availability:** Data and systems must be reliably accessible to authorized personnel. Redundant systems, backup strategies, and recovery plans ensure uninterrupted service.

- **Responsibility:** Duties for data protection are distinctly allocated across the organization. All individuals managing data are accountable for its safekeeping.
- **Adherence:** Security controls are crafted to comply with legal and regulatory mandates in Curaçao and globally, aligning with standards like ISO/IEC 27001 and leading practices in the gaming industry.

Security Architecture

Network and System Defense

The Company implements a tiered defense strategy to counter threats from both external and internal sources. This includes firewalls, intrusion detection and prevention mechanisms, DDoS countermeasures, and encrypted communication links. All gaming and payment interactions are protected with state-of-the-art encryption methods.

Access Governance

Access to information follows the least privilege principle. Each role receives only the permissions essential for its tasks, enforced via multi-factor authentication and rigorous session monitoring. Access privileges are reassessed periodically, with immediate revocation upon termination of employment or engagement.

Data Security

Personal and financial information is encrypted during storage and transit. Robust encryption protocols are utilized to ensure data remains secure even if accessed improperly. Sensitive data elements are anonymized where practicable to limit identification risks.

Software and Device Protection

The Company preserves the reliability of its gaming applications and systems through secure development methodologies. Periodic penetration tests, vulnerability checks, and external certifications are performed to address potential flaws. All devices, including those used by employees, are governed by mobile device management and endpoint security tools.

Surveillance and Evaluation

The Company actively tracks its systems for anomalous behavior. Security incidents are recorded in a centralized system for real-time monitoring and analysis. Logs are retained in protected, high-availability storage and reviewed by internal auditors. Consistent audits verify ongoing compliance with internal guidelines and external regulations.

Partner Compliance

Third-party providers and vendors delivering critical services must align with the Company's security expectations. Comprehensive due diligence is conducted prior to engagement, and

contracts enforce strict data handling requirements. Regular reviews ensure continued adherence to these standards.

Staff Duties

Information security is a shared obligation for all individuals associated with the Company. Employees and contractors must undergo regular training on cybersecurity, data safeguarding, and anti-money laundering protocols. They are obligated to report any incidents or suspected vulnerabilities in information systems immediately.

Pre-employment vetting, including integrity and background verifications, is required for personnel handling sensitive data or system administration roles. Staff are barred from using unapproved devices or applications, with only Company-approved equipment permitted for accessing internal networks.

Incident Handling and Breach Response

The Company maintains a formalized incident response framework to address events that may threaten information security. This framework ensures that:

1. Incidents are promptly detected and isolated.
2. Investigations determine the origin and scope of the breach.
3. Regulatory authorities, affected users, and relevant parties are informed swiftly and transparently, per legal stipulations.
4. Restoration efforts return systems to normal functionality without undue delay.
5. Lessons derived are integrated into revised protocols to avoid future incidents.

Risk Assessment

Information security risks are evaluated on a continuous basis. Thorough assessments are conducted annually and following significant technological or operational shifts. Independent penetration testing, system reviews, and gaming software validations are integral to the risk assessment process.

Identified risks are logged in a detailed register, ranked by severity and probability, and addressed through targeted technical and organizational solutions. The process also addresses emerging dangers, such as fraud, digital attacks, and exploitation of gaming platforms.

Compliance and Accountability

This Policy is binding. Employees who breach its terms may face disciplinary actions, up to and including termination. Violations by suppliers or partners may lead to contract termination and, where applicable, notification to regulatory bodies.

The Company understands that its gaming license relies on secure, transparent, and responsible operations. Compliance with this Policy is thus a prerequisite for employment, collaboration, and ongoing business activities.

Evaluation and Ongoing Refinement

This Policy is reviewed at least annually, or more frequently if regulatory updates, significant technological advancements, or notable incidents indicate a need for enhancement.

Amendments are documented, ratified by senior leadership, and shared with all employees and partners.

Information security is an evolving discipline requiring constant improvement. By embracing innovative technologies, responding to new threats, and cultivating a security-aware culture, the Company ensures its protective measures remain robust and its operations trustworthy.

Oversight

The Board of Directors bears ultimate responsibility for the security of the Company's information and systems. The Chief Information Security Officer is tasked with executing and supervising this Policy, ensuring sufficient resources, processes, and safeguards are in place.

Independent internal and external audits are performed to confirm compliance and provide confidence to regulators, stakeholders, and players that the Company upholds the highest standards of integrity and protection.

Approved by  **Serhiy Podolinskyi**
Director of Geosix B.V.

