

Information Security Policy

For <http://clickpari.com> LOTOSTORM B.V.

01.09.2025

Approved by: Board of Directors

Policy Vision and Rationale

<http://clickpari.com>, overseen by LOTOSTORM B.V., delivers online gaming services that depend on the steadfast and protected processing of sensitive information. The Company regards personal data, monetary records, gaming interactions, and operational files as essential assets requiring top-tier protection.

The objective of this Information Security Policy is to create a cohesive strategy for defending these valuable resources. It strives to maintain the privacy, accuracy, and accessibility of data, while enabling the Company to offer gaming services with robust security, openness, and ethical standards. Through this Policy, LOTOSTORM B.V. commits to meeting all relevant data protection regulations, anti-money laundering rules, and gaming industry guidelines, while aligning with globally respected security benchmarks.

Scope of Coverage

This Policy applies to every individual linked to the Company, including permanent staff, temporary hires, consultants, and external service providers. It oversees all technological components—such as software platforms, server networks, and hardware systems—utilized in gaming operations, alongside supporting elements like data storage facilities, backup mechanisms, and disaster recovery frameworks.

The Policy includes all data managed by the Company, irrespective of its format, encompassing player profiles, financial exchanges, business documents, technical logs, and regulatory submissions. It also reaches third-party suppliers providing critical support to the gaming platform, mandating that they maintain equivalent security protocols.

Employee Roles and Training

Information security is a collective duty for all individuals affiliated with the Company. All employees and contractors must participate in ongoing education on cybersecurity, data safeguarding, and anti-money laundering protocols, ensuring they are equipped to protect sensitive information. Any security breaches or potential vulnerabilities must be reported immediately.

Prior to employment, individuals handling sensitive data or managing systems undergo thorough background and integrity checks. The use of unauthorized devices or software is strictly forbidden, with only Company-approved equipment allowed for accessing internal networks.

Security Infrastructure

Network and System Resilience

LOTOSTORM B.V. adopts a multi-level defense strategy to shield its systems from both external and internal risks. This includes advanced firewalls, intrusion monitoring and prevention tools, DDoS protection, and encrypted communication lines. All gaming and payment activities are safeguarded with the latest encryption technologies.

Access Management

Information access is regulated under a least-privilege framework. Each role is granted only the permissions necessary for its tasks, secured by multi-factor authentication and rigorous session oversight. Access rights are evaluated regularly, with immediate revocation upon termination of employment or contracts.

Data Confidentiality Measures

Personal and financial information is encrypted during storage and transfer. State-of-the-art encryption techniques ensure data remains secure even if accessed without authorization. Sensitive identifiers are masked where possible to minimize identification risks.

Software and Device Integrity

The Company preserves the reliability of its gaming applications and systems through secure development practices. Frequent penetration tests, vulnerability scans, and external certifications are performed to address potential flaws. Employee devices are controlled with mobile device management and endpoint security solutions.

Oversight and Logging

The Company actively surveils its systems for unusual activity. Security incidents are tracked in a centralized system for real-time analysis and response. Logs are stored in protected, high-availability environments and reviewed by internal auditors, with periodic assessments ensuring compliance with internal and external standards.

Vendor Compliance

External partners and suppliers delivering essential services must align with the Company's security expectations. Pre-engagement due diligence is required, and contracts enforce strict data handling obligations. Ongoing evaluations confirm adherence to these requirements.

Governance Oversight

The Board of Directors bears final responsibility for the security of the Company's information assets and technological infrastructure. The Chief Information Security Officer

(CISO) is charged with implementing and monitoring this Policy, ensuring adequate resources, processes, and safeguards are in place.

To affirm compliance and build trust with regulators, stakeholders, and users, the Company conducts regular independent internal and external audits, demonstrating its commitment to the highest levels of integrity and protection.

Risk Assessment and Mitigation

The Company performs continuous evaluations to identify and manage information security risks. In-depth reviews are conducted annually and following significant technological or operational changes, incorporating independent penetration testing, system audits, and gaming software validations.

Identified risks are documented in a detailed inventory, prioritized by severity and likelihood, and addressed through tailored technical and organizational responses. This process also accounts for emerging threats, such as financial scams, cyberattacks, and gaming platform exploitation.

Incident Response and Recovery

LOTOSTORM B.V. maintains a structured incident response procedure to address events that may jeopardize information security. This procedure ensures:

1. Rapid detection and isolation of incidents.
2. Comprehensive investigations to determine origins and consequences.
3. Timely and clear notifications to regulators, affected parties, and stakeholders, as mandated by law.
4. Efficient restoration of normal operations.
5. Incorporation of insights into revised protocols to prevent future incidents.

Compliance and Accountability

This Policy is compulsory. Employees who breach its terms may face disciplinary actions, up to and including dismissal. Violations by vendors or partners may result in contract termination and, where necessary, referral to regulatory bodies.

The Company acknowledges that its gaming license relies on secure, transparent, and responsible practices. Adherence to this Policy is thus a core requirement for employment, partnerships, and ongoing operations.

Policy Evaluation and Advancement

This Policy is assessed at least annually, or more often if regulatory changes, technological shifts, or significant incidents highlight areas for enhancement. Updates are recorded, approved by senior leadership, and shared with all staff and partners.

Information security is an evolving practice demanding constant improvement. By investing in innovative technologies, adapting to new risks, and nurturing a security-conscious culture, the Company ensures its defenses remain solid and its services trustworthy.

Approved by  **Volodymyr Zhukovskiy**
Director of LOTOSTORM B.V.

