

Information Security Policy

For <http://pongbet88.com>

KREVETKA B.V.

Effective Date: 01.09.2025

Approved by: Board of Directors

Policy Objectives and Context

<http://pongbet88.com>, under the stewardship of KREVETKA B.V., provides online gaming experiences that hinge on the reliable and protected management of critical data. The Company views personal details, financial transactions, gaming activities, and administrative records as vital assets deserving the highest degree of safeguarding.

This Information Security Policy establishes a robust blueprint to shield these resources, ensuring their confidentiality, integrity, and accessibility. Its primary aim is to support the Company's mission to deliver gaming services with unwavering security, clarity, and accountability. By endorsing this Policy, KREVETKA B.V. pledges to adhere to all pertinent data privacy laws, anti-money laundering directives, and gaming regulations, while embracing globally acknowledged security protocols.

Scope of Application

This Policy governs all individuals associated with the Company, including full-time staff, temporary workers, advisors, and external collaborators. It encompasses all technological assets—such as software platforms, server networks, and operational hardware—used in gaming operations, along with ancillary resources like data storage units, contingency backups, and emergency recovery setups.

All data processed by the Company, regardless of its medium, falls under this Policy's purview. This includes customer identities, payment records, business documentation, technical logs, and reports submitted for regulatory oversight. Furthermore, the Policy extends to third-party vendors supplying key services or products to the gaming platform, requiring them to uphold identical security commitments.

Governance Structure

The Board of Directors holds ultimate authority over the security of the Company's information assets and technological infrastructure. The Chief Information Security Officer (CISO) is entrusted with the execution and supervision of this Policy, ensuring the allocation of necessary resources, the development of effective procedures, and the implementation of stringent controls.

To validate compliance and instill confidence among regulators, stakeholders, and users, the Company commissions regular independent internal and external audits. These evaluations



confirm that KREVETKA B.V. maintains the pinnacle of ethical and protective standards in its operations.

Foundational Security Principles

The Company's security strategy is anchored in the following core tenets:

- **Privacy Protection:** Confidential data must be insulated from unauthorized scrutiny or release. Access is restricted to essential business functions, bolstered by rigorous authentication and encryption safeguards.
- **Data Reliability:** Information must remain precise, unaltered, and credible. Systems are engineered with mechanisms to detect and prevent interference, validated through periodic third-party reviews.
- **Operational Access:** Data and systems must be readily available to authorized personnel. Redundant configurations, data backups, and recovery protocols guarantee seamless service continuity.
- **Duty of Care:** Accountability for data security is explicitly delegated across the organization. Every individual interacting with information bears responsibility for its protection.
- **Regulatory Alignment:** Security measures are tailored to fulfill legal and regulatory obligations in Curaçao and worldwide, drawing on frameworks like ISO/IEC 27001 and industry-leading practices in online gaming.

Risk Identification and Mitigation

The Company conducts ongoing assessments to identify and address information security risks. Detailed evaluations occur annually and following significant updates to technology or business processes. These assessments incorporate independent penetration testing, infrastructure audits, and certifications of gaming software.

Documented risks are cataloged in a systematic ledger, ranked by potential impact and probability, and neutralized through targeted technical and administrative interventions. The risk management approach also anticipates evolving challenges, such as financial fraud, cyber intrusions, and the misuse of gaming platforms, ensuring proactive defense strategies.

Security Measures

Network and System Fortification

KREVETKA B.V. deploys a multi-tiered defense mechanism to shield its systems from external and internal risks. This includes advanced firewalls, intrusion detection and prevention technologies, DDoS resistance, and encrypted data channels. All gaming and financial interactions are secured with contemporary encryption standards.



Access Regulation

Information access is governed by a minimal privilege model. Each position is granted only the permissions required for its role, enforced via multi-factor authentication and tight session management. Access credentials are reviewed at regular intervals, with immediate revocation upon the end of employment or contractual relationships.

Data Encryption and Anonymity

Personal and financial data are encrypted during storage and transmission. High-strength encryption protocols ensure data remains indecipherable even in breach scenarios. Sensitive data points are anonymized where feasible to reduce identification exposure.

Software and Device Safeguards

The Company upholds the stability of its gaming applications and systems through secure coding standards. Ongoing penetration testing, vulnerability assessments, and external validations are conducted to rectify potential weaknesses. Employee devices are monitored with mobile management tools and endpoint security solutions.

Continuous Monitoring and Review

The Company maintains constant vigilance over its systems for irregular activity. Security incidents are recorded in a unified platform for immediate detection and analysis. Logs are stored in fortified, high-availability archives and scrutinized by internal auditors. Routine audits ensure alignment with internal policies and external mandates.

Vendor Accountability

Third-party providers of essential services must meet the Company's security criteria. Pre-engagement due diligence is mandatory, and contractual agreements stipulate rigorous data handling expectations. Periodic evaluations confirm ongoing compliance with these standards.

Incident Response and Recovery Protocols

KREVETKA B.V. maintains a structured incident response strategy to manage events that may undermine information security. This strategy ensures:

1. Prompt identification and containment of incidents.
2. Thorough investigations to determine causes and effects.
3. Timely and transparent notifications to regulators, affected parties, and stakeholders, as required by law.
4. Swift recovery actions to resume normal operations.
5. Integration of lessons learned into enhanced procedures to prevent future occurrences.

Employee Conduct and Training

Every individual affiliated with the Company shares the responsibility for information security. Staff and contractors must complete periodic training on cybersecurity, data protection, and anti-money laundering practices. They are required to report any security incidents or potential vulnerabilities without delay.

Pre-employment screening, encompassing integrity and background checks, is conducted for employees handling sensitive data or managing systems. Use of unauthorized devices or software is prohibited, with only Company-sanctioned equipment permitted for internal system access.

Compliance and Disciplinary Measures

This Policy is enforceable. Employees who contravene its terms may face disciplinary actions, ranging from warnings to termination. Breaches by vendors or partners may lead to contract dissolution and, where necessary, escalation to regulatory authorities.

The Company recognizes that its gaming license hinges on secure, transparent, and responsible conduct. Compliance with this Policy is therefore a fundamental condition of employment, partnership, and sustained operations.

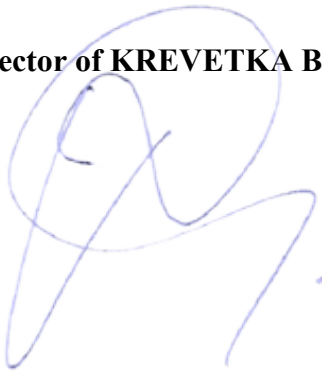
Policy Review and Evolution

This Policy undergoes evaluation at least annually, or more frequently in response to regulatory shifts, significant technological advancements, or major incidents necessitating improvement. Revisions are recorded, endorsed by senior executives, and disseminated to all staff and collaborators.

Information security is a dynamic endeavor requiring ongoing enhancement. Through investment in cutting-edge technologies, adaptation to emerging threats, and the promotion of a security-focused culture, the Company ensures its defenses remain resilient and its services deserving of trust.

Approved by _____ **Roland Eduard Gertruda de Mei**

Director of KREVETKA B.V.

A handwritten signature in blue ink, consisting of a large, stylized 'R' followed by a long horizontal stroke and a small dot at the end.