

Information Security Policy

For MELBET.COM (Operated by PELICAN ENTERTAINMENT B.V.)

Effective Date: 01.09.2025

Endorsed by: The Board of Directors

1. Purpose and Context

[MELBET.COM](#) (the "Website"), operated by PELICAN ENTERTAINMENT B.V. in Curaçao (reg. number: 134359, reg. address: 1, Dr. H. Fergusonweg, Willemstad, Curaçao), delivers online gaming services (licensed by Curacao Gaming Authority in accordance with the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) (NOOGH), License number: OGL/2024/561/0554) that depend on the reliable and secure management of sensitive information. The Company is fully aware that the protection of personal details, payment records, business transactions, and operational documents is fundamental to both its reputation and its license to operate. Safeguarding these assets is not only a technical requirement but also a matter of trust between the Company and its customers.

The objective of this charter is to outline a clear and unified approach to managing information security risks across the entire organization. By defining this framework, the Company ensures that confidentiality, accuracy, and availability of data remain uncompromised, while at the same time guaranteeing service continuity. In doing so, the Company also demonstrates its full commitment to meeting all legal requirements in areas such as data protection, anti-money laundering obligations, and sector-specific gaming regulations. These commitments are not viewed as burdens but as essential components of responsible and sustainable business operations.

2. Scope and Applicability

The scope of this policy extends to every person and entity involved in the Company's activities. Employees, independent contractors, external consultants, and third-party providers are all bound by the same responsibilities when handling information. The systems covered include in-house applications, servers, cloud infrastructure, disaster recovery facilities, and all related technical resources that enable the delivery of gaming services.

Equally important, the scope does not stop with internal staff or technology. All categories of information, such as player registration details, financial data, corporate records, compliance reports, and system-generated logs—are included, regardless of whether they are digital or physical. Suppliers and external partners are also explicitly required to comply with the Company's security standards. The expectation is clear: every party involved in the operation of the Website must adopt the same level of diligence when protecting data. By ensuring this consistency, the Company establishes a culture in which security responsibilities are universally recognized and applied.

3. Foundational Security Principles

The Company's information security practices are built on a set of guiding principles that inform all decisions and measures. The first is confidentiality, which means that sensitive information must remain shielded from unauthorized access. Data can only be used for legitimate business purposes, and measures such as encryption, access controls, and strong authentication are deployed to make this possible.

Integrity is the second principle, reflecting the Company's determination to ensure data accuracy and completeness. Systems are designed to prevent and detect tampering, while regular validation procedures and independent checks help guarantee that information remains reliable. The third principle is availability, which emphasizes that customers and staff must be able to access services without disruption. Redundant systems, backups, and disaster recovery strategies have been put in place to minimize downtime.

Finally, accountability and compliance round out the Company's guiding framework. Every employee and partner has defined responsibilities for safeguarding data, and the Company's measures are aligned with both Curaçao regulations and global standards such as ISO/IEC 27001. This set of values is not treated as theory but as a living foundation upon which the Company builds its everyday operations.

4. Safeguards and Security Controls

Security is implemented through multiple layers of defense. At the infrastructure level, protections include firewalls, intrusion detection systems, DDoS prevention, and encrypted channels for all communication. These technical measures ensure that both gaming transactions and payment processes are safeguarded against interference. Importantly, the approach recognizes that no single control is sufficient, which is why multiple overlapping protections are maintained.

Access governance is equally critical. Employees and contractors are granted the least amount of access necessary for their roles. This principle of least privilege is supported by multi-factor authentication, strong session controls, and periodic reviews of user rights. Access is withdrawn immediately when a person's engagement ends, reducing opportunities for misuse. In addition to access management, data itself is protected at every stage. All sensitive data, whether stored or transmitted, is encrypted using modern algorithms. In some cases, data is pseudonymized to reduce the possibility of re-identification. Even in the unlikely event of unauthorized access, these measures ensure the information is unusable to outsiders.

Another safeguard lies in application and endpoint security. The Company's gaming software is developed with secure coding practices, and independent experts carry out regular vulnerability assessments and penetration tests. Employee devices are subject to strict endpoint protection and mobile device management policies. These controls acknowledge that security is only as strong as the weakest link, and that both software and hardware must be equally protected. The Company also extends its security expectations to suppliers and partners. Formal due diligence is performed before contracting, and partners must agree to handle information according to strict requirements. Compliance is then monitored continuously through audits and reviews.

5. Responsibilities of People

Information security is not confined to technology; it also relies on the awareness and actions of people. Every employee, contractor, and consultant is expected to contribute actively to protecting data. This begins with training programs that cover cybersecurity awareness, data handling, and anti-money laundering procedures. Staff are encouraged to report suspicious activity or weaknesses immediately so that corrective measures can be taken without delay.

Before recruitment into sensitive roles, individuals undergo background and integrity checks. Once employed, they are bound by clear rules that prohibit the use of unauthorized devices, applications, or personal accounts for work purposes. Only approved and monitored equipment may connect to the Company's systems. This strict approach prevents accidental or intentional breaches and reinforces a shared understanding that every individual has a part to play in maintaining security. By placing people at the heart of its security culture, the Company recognizes that human vigilance can often prevent incidents that technology alone cannot stop.

6. Incident Response and Recovery

Despite robust controls, the Company accepts that incidents may still occur. For this reason, a formal incident response plan has been developed to ensure that any security event is contained quickly and effectively. The plan covers detection, investigation, communication, and recovery. When an incident arises, the priority is to identify its nature, contain the threat, and begin a structured investigation into its cause and impact.

Transparency is a key part of this process. Regulatory authorities, affected customers, and other stakeholders are informed without unnecessary delay, and communication is handled openly in line with legal requirements. At the same time, recovery actions are implemented to restore systems to normal functioning. Once operations are stable, the Company conducts a review of lessons learned. These insights are then used to update processes and prevent similar issues from recurring. In this way, the Company treats each incident not just as a problem but as an opportunity to further strengthen its resilience.

7. Risk Assessment and Management

Security risks are not static; they evolve continuously with new technologies, changing customer behavior, and emerging criminal tactics. To manage this dynamic environment, the Company performs regular risk assessments. Comprehensive reviews take place annually and whenever significant changes occur in operations or infrastructure.

A structured risk register is maintained to record all identified threats, categorizing them by likelihood and potential impact. Mitigation strategies are then prioritized, ensuring that resources are directed toward the most critical issues. Independent audits, penetration testing, and third-party certifications provide additional assurance that risks are being appropriately managed. Special attention is given to emerging threats such as cybercrime, fraud, and the misuse of gaming platforms. This proactive approach ensures that risks are not only identified but also addressed before they cause harm.

8. Compliance, Enforcement, and Accountability

Compliance with this charter is mandatory for all parties associated with the project.. Employees who breach its provisions may face disciplinary action, including dismissal.

Contractors and partners who fail to comply risk contract termination and possible reporting to regulators. These enforcement measures are not taken lightly but reflect the seriousness with which the Company treats information security.

At the same time, compliance is not viewed purely as an obligation. It is also a business necessity. The Company's gaming license, its reputation with customers, and its relationship with regulators all depend on transparent and responsible conduct. For this reason, adherence to the charter is considered a condition of employment and partnership. The message is clear: security and compliance are not separate from business: they are fundamental to its survival.

9. Review and Ongoing Improvement

This policy is reviewed at least once every year, and more frequently if circumstances demand it. Triggers for updates include new legal requirements, major technological developments, or lessons learned from incidents. Any changes are documented, approved at senior management level, and communicated across the organization to ensure everyone is aware of their responsibilities.

Security is not a static checklist but a process of ongoing improvement. The Company continues to invest in modern technologies, refine its processes, and strengthen its culture of awareness. By adapting to evolving threats and remaining proactive, the Company ensures that it maintains a high level of resilience. The ongoing commitment to improvement demonstrates that protecting information is not simply a compliance exercise, it is an enduring responsibility to customers, regulators, and stakeholders.

10. Governance and Oversight

The success of an information security program depends not only on technical defenses but also on a well-defined governance structure. The Company maintains a clear chain of responsibility that begins with the Board of Directors and extends throughout the organization. Senior management is accountable for establishing the strategic direction of information security, approving policies, and allocating the resources necessary to implement them effectively. They set the tone at the top by emphasizing that security is a business priority, not simply a technical concern.

A cross-functional security committee has been established to oversee the application of this charter in daily operations. This committee meets regularly to review incidents, evaluate risk assessments, and recommend updates to policies or controls. It includes representatives from technology, compliance, operations, and legal functions, ensuring

that decisions reflect diverse perspectives. The committee also acts as the main forum for escalating issues that require executive attention.

Operational governance extends further through defined roles and responsibilities at the departmental level. Managers are tasked with ensuring that their teams understand security expectations, complete required training, and apply the correct practices in their workflows. Internal auditors provide independent oversight by testing whether controls are functioning as intended, while external auditors and regulators offer an additional layer of assurance.

Through this governance framework, the Company ensures that information security is not an isolated function but a collective responsibility supported by leadership, embedded in operations, and verified through independent review. By assigning responsibility at every level, the Company creates an environment where accountability is clear and continuous improvement is expected.

This Information Security Policy has been reviewed, endorsed, and formally approved by the Company's governing body. By signing below, the undersigned confirm their commitment to uphold the principles and requirements set out in this policy and to ensure that all employees, contractors, and partners adhere to its provisions.

For and on behalf of PELICAN ENTERTAINMENT B.V.

A handwritten signature in blue ink, consisting of a stylized 'S' followed by a horizontal line and a small flourish.

Solutions for Management and Employment Support N.V.,

Director