

Information Security Policy

For <https://marafon.bet>

ENCODE DIGITAL B.V.

Effective Date: 01.09.2025

Approved by: Board of Directors

Introduction and Objective

<https://marafon.bet>, managed by ENCODE DIGITAL B.V., engages in online gaming operations that depend on the secure and uninterrupted management of sensitive data. The Company acknowledges that personal information, financial data, gaming transactions, and operational records constitute valuable assets requiring the utmost protection.

The purpose of this Information Security Policy is to establish a cohesive framework for safeguarding these assets. It seeks to ensure the confidentiality, integrity, and accessibility of information while supporting the Company's ability to deliver gaming services in a secure, transparent, and accountable manner. Through this Policy, the Company reaffirms its dedication to adhering to all relevant data protection, anti-money laundering, and gaming industry regulations, as well as aligning with globally accepted standards of excellence.

Scope

This Policy encompasses all individuals associated with the Company, including employees, contractors, consultants, and external service providers. It applies to all systems, applications, servers, and infrastructure utilized in delivering gaming services, along with associated facilities such as data centers, backup systems, and disaster recovery mechanisms.

The Policy addresses all data processed by the Company, irrespective of its format, including player personal information, financial dealings, corporate documentation, system logs, and reports generated for regulatory or compliance purposes. It also extends to suppliers providing critical goods or services to support the gaming platform, ensuring that external collaborators maintain equivalent security standards.

Guiding Principles

The Company's information security efforts are underpinned by the following principles:

- **Confidentiality:** Sensitive information shall be shielded from unauthorized access or disclosure. Access is granted solely based on operational need, reinforced by robust authentication protocols and encryption.

- **Integrity:** Data must remain accurate, intact, and reliable. Systems are engineered to detect and prevent alterations, supported by independent testing and verification processes.
- **Availability:** Information and systems must be reliably accessible to authorized personnel. Redundancy, backup protocols, and disaster recovery strategies ensure operational continuity.
- **Accountability:** Responsibilities for information protection are explicitly assigned throughout the organization. Every individual handling data is held responsible for its safeguarding.
- **Compliance:** Security practices are tailored to meet legal and regulatory obligations in Curaçao and beyond, reflecting standards such as ISO/IEC 27001 and best practices within the online gaming industry.

Security Framework

Network and Infrastructure Safeguards

The Company adopts a multi-layered strategy to protect its systems from internal and external threats. This includes firewalls, intrusion detection and prevention tools, DDoS protection, and encrypted communication channels. All gaming and payment transactions are secured with cutting-edge encryption technologies.

Access Management

Access to information adheres to the principle of least privilege. Each role is allocated only the access required for its functions, enforced through multi-factor authentication and stringent session oversight. Access privileges are reviewed regularly, and all rights are revoked immediately upon termination of employment or engagement.

Data Safeguarding

Personal and financial data are encrypted during storage and transmission. Advanced encryption standards are applied to ensure data remains secure even if accessed without authorization. Where feasible, sensitive identifiers are pseudonymized to minimize re-identification risks.

Application and Device Security

The Company maintains the reliability of its gaming software and systems through secure coding practices. Routine penetration testing, vulnerability assessments, and third-party certifications are conducted to identify and resolve weaknesses. All endpoints, including employee devices, are managed with mobile device oversight and endpoint security solutions.

Monitoring and Oversight

The Company actively monitors its systems for unusual activity. Security incidents are logged in a centralized system that facilitates real-time detection and analysis. Logs are stored in secure, highly available locations and examined by internal auditors. Periodic audits ensure continuous adherence to internal policies and external mandates.

Vendor Management

Vendors and third parties providing essential services must comply with the Company's security benchmarks. Thorough due diligence is conducted prior to engagement, and contractual agreements impose rigorous requirements for data handling. Ongoing evaluations verify compliance with these standards.

Employee Obligations

Ensuring information security is a duty shared by all individuals affiliated with the Company. Employees and contractors must participate in regular training on cybersecurity, data privacy, and anti-money laundering protocols. They are required to promptly report any incidents or potential vulnerabilities in information systems.

Pre-employment vetting, including integrity and background screenings, is mandatory for staff handling sensitive data or managing systems. Employees are forbidden from using unapproved devices or software, with only Company-managed equipment permitted for accessing internal networks.

Incident Response and Breach Handling

The Company maintains a structured incident response plan to manage events that may jeopardize information security. This plan ensures that:

1. Incidents are swiftly identified and contained.
2. Investigations determine the cause and extent of impact.
3. Regulatory authorities, affected clients, and relevant stakeholders are notified promptly and transparently, in line with legal obligations.
4. Recovery measures restore normal operations without undue delay.
5. Insights gained are integrated into revised procedures to prevent future occurrences.

Risk Management

Information security risks are evaluated continuously. Detailed assessments are performed annually and following significant technological or operational changes. Independent penetration testing, system audits, and gaming software validations are integral to the risk management framework.

Identified risks are documented in a formalized register, prioritized by impact and probability, and addressed through suitable technical and organizational measures. The process also accounts for emerging threats, such as fraud, cyberattacks, and misuse of gaming platforms.

Compliance and Enforcement

This Policy is compulsory. Violations by employees may lead to disciplinary actions, including termination. Breaches by suppliers or partners may result in contract cancellation and, where necessary, notification to regulatory bodies.

The Company recognizes that its gaming license hinges on secure, transparent, and responsible operations. Accordingly, compliance with this Policy is a prerequisite for employment, partnerships, and ongoing business activities.

Review and Ongoing Enhancement

This Policy is evaluated at least annually, or more often if regulatory changes, major technological updates, or significant incidents highlight areas for improvement. Revisions are recorded, endorsed by senior leadership, and disseminated to all employees and partners.

Information security is a dynamic process of continual improvement. Through investment in innovative technologies, adaptation to evolving risks, and promotion of a security-conscious culture, the Company ensures its defenses remain robust and its operations trustworthy.

Governance

The Board of Directors holds ultimate responsibility for the security of the Company's information and systems. The Chief Information Security Officer oversees the implementation and management of this Policy, ensuring adequate resources, processes, and controls are in place.

Independent internal and external audits are conducted to confirm compliance and provide assurance to regulators, stakeholders, and players that the Company operates with the highest standards of integrity and protection.

Approved by



Andreou Theoklis Director of ENCODE DIGITAL B.V.