

Information Security Policy

Company name: **GAMEPLAY INTERNATIONAL B.V.**
Effective Date: **01 September 2025**
Approved and Signed by: **The Director, (SMES) Solutions for Management and Employment Support N.V.**

Signature:



1. Introductory Statement

GAMEPLAY INTERNATIONAL B.V., incorporated under Curaçao law (registration no. 148409) and located at 1, Dr. Henri Fergusonweg, Willemstad, Curacao, operates digital gaming platforms. The company holds a valid license (No. OGL/2024/511/0630) from the Curaçao Gaming Authority in accordance with the National Ordinance on Offshore Games of Hazard.

Because our operations involve continual handling of sensitive data, such as customer identities, financial records, and internal business information, robust protection is vital. This policy establishes a structured approach to ensuring data confidentiality, reliability, and accuracy. It demonstrates our compliance with legislation and international standards while reinforcing our position as a trusted gaming operator.

2. Scope of Application

This framework applies to every individual and organization working with GAMEPLAY INTERNATIONAL B.V. Employees, contractors, consultants, vendors, and service partners are all within scope. The rules cover not only people but also all relevant technology assets including hardware, software, cloud platforms, and recovery environments.

The coverage extends to all categories of information assets: customer details, payment records, compliance submissions, regulatory filings, and system logs.

Partners and suppliers must meet the same expectations, ensuring consistent protection both internally and externally.

3. Core Security Principles

Our approach to security is anchored in key principles. Protecting personal data from unauthorized use is a top priority. To achieve this, we employ strict access restrictions, multi-factor authentication, and encryption at various stages.

Safeguarding data integrity ensures information remains trustworthy and accurate. Equally, the stability and reliability of our services are essential. This is why we maintain redundant systems, resilient backup strategies, and tested recovery plans. Responsibility for security rests with everyone in the organization, making it a collective duty. Above all, we align with local and international regulatory standards, guaranteeing compliance and operational legitimacy.

4. Safeguards and Administrative Controls

Technical Infrastructure Protection	We implement a defense-in-depth strategy, using firewalls, intrusion prevention/detection systems, DDoS protection, and encrypted communication channels for all critical transmissions, including payments and game traffic
Identity and Access Governance	Permissions follow the “least privilege” model, granting only the access needed for each role. Authentication mechanisms are strong, activity is monitored, and rights are reviewed frequently. When an employee leaves or changes position, access is immediately revoked
Data Handling and Protection	Sensitive data is always encrypted both in storage and during transfer. Where possible, personal identifiers

	are masked or pseudonymized to reduce exposure risks
Application and Device Security	Our applications and gaming platforms follow secure development practices and undergo continuous independent testing, including penetration assessments. All devices used to access systems are subject to endpoint protection and mobile device management controls
Monitoring and Assurance	We operate centralized monitoring and logging tools to detect unusual activity. Regular reviews and audits confirm the effectiveness of our controls and allow timely adjustments
Third-Party Oversight	Vendors are carefully vetted before engagement. They must contractually agree to comply with our security standards and undergo periodic reassessment to confirm alignment

5. Employee and Contractor Duties

All staff and contractors are accountable for safeguarding company assets. Completion of training on cybersecurity, anti-fraud awareness, and compliance requirements is mandatory. Any suspicious behavior or system weaknesses must be reported promptly.

Roles that involve access to critical information require background checks. Only company-issued and managed devices may be used for work activities, with personal hardware or unauthorized applications strictly prohibited.

6. Incident Response

We maintain a structured incident response plan to ensure swift detection, containment, and remediation of security events. Each case is investigated thoroughly, with root causes analyzed and addressed.

When an incident affects customers, regulators, or partners, we provide timely and transparent notifications. Services are restored as quickly as possible, and lessons learned are incorporated into updated security practices.

7. Risk Management

Risk identification and mitigation is an ongoing responsibility. We rely on audits, assessments, and certification programs to uncover vulnerabilities. Risks are cataloged in a central register, assessed for likelihood and impact, and treated accordingly.

In addition, we track emerging threats such as cybercrime and system abuse to remain prepared against evolving risks.

8. Compliance and Enforcement

Observance of this policy is mandatory. Employees who fail to follow its provisions may face disciplinary action, including termination. Business partners or vendors who do not comply may have their agreements suspended or terminated.

9. Continuous Improvement

We are committed to refining our security framework on an ongoing basis. Feedback from audits, lessons from incidents, and advances in technology all inform the evolution of our defenses.

10. Oversight and Governance

Ultimate accountability for information security rests with the Company's leadership. A defined supervisory structure ensures proper governance, with responsibilities delegated across relevant functions for effective oversight and decision-making.