

Information Security Policy

For <https://portebet.com> DOUBLED B.V.

Effective Date: 01.09.2025

Approved by: Board of Directors

Introduction and Purpose

DOUBLED B.V., operating <https://portebet.com>, engages in online gaming activities that involve the constant processing of sensitive data. The Company acknowledges that personal information, financial details, gaming records, and internal documents constitute critical assets that must be safeguarded with the highest diligence.

This Information Security Policy establishes a comprehensive framework to ensure such assets are protected. Its purpose is to maintain confidentiality, integrity, and availability of information, while preserving the Company's ability to deliver gaming services in a secure, transparent, and responsible manner. Through this Policy, the Company further commits to comply with all relevant data protection, anti-money laundering, and gaming industry regulations, while adhering to internationally recognized security standards.

Scope

This Policy applies to all individuals engaged by DOUBLED B.V., including employees, contractors, consultants, and third-party service providers. It governs all applications, servers, networks, and infrastructure supporting the gaming operations, as well as associated facilities such as data centers, backups, and disaster recovery environments.

The Policy extends to all forms of information handled by the Company, including player data, financial transactions, corporate documentation, system logs, and regulatory reports. It also encompasses suppliers and external partners whose services are integral to the platform, ensuring they meet equivalent security standards.

Guiding Principles

The Company's approach to information security is guided by the following principles: - **Confidentiality:** Sensitive data must be shielded from unauthorized access or disclosure, with access rights granted strictly on a need-to-know basis and reinforced by authentication and encryption. - **Integrity:** Data must remain reliable, accurate, and complete. Systems are designed to prevent tampering, with independent validation and testing. - **Availability:** Information and systems must be reliably accessible to authorized parties, supported by redundancy, backups, and recovery planning. - **Accountability:** Information protection responsibilities are clearly allocated across the organization, with each individual accountable for safeguarding data. - **Compliance:** Security measures align with Curaçao and



international regulatory requirements, and reflect best practices such as ISO/IEC 27001, alongside online gaming sector standards.

Security Framework

Network and Infrastructure Protection

A multi-layered defense strategy is in place to counter threats. This includes firewalls, intrusion detection/prevention, DDoS mitigation, and secure encrypted communication channels for both gaming and payment operations.

Access Control

Access rights follow the principle of least privilege, enforced through multi-factor authentication and session controls. Permissions are regularly reviewed, and revoked immediately upon termination of employment or contract.

Data Protection

Personal and financial information is encrypted at rest and in transit. Pseudonymization is used wherever feasible to reduce re-identification risks.

Application and Endpoint Security

The integrity of the Company's gaming software is ensured through secure development, regular penetration testing, vulnerability assessments, and independent certification. All endpoints are monitored and managed with protective systems.

Monitoring and Auditing

Real-time monitoring and centralized logging enable prompt detection of suspicious activities. Logs are retained securely and reviewed by auditors. Internal and external audits verify compliance and robustness.

Supplier Oversight

Suppliers are subject to due diligence, contractual obligations, and regular assessments to confirm adherence to the Company's security standards.

Employee Responsibilities

Every individual working with DOUBLED B.V. is responsible for information security. Staff and contractors undergo regular training on cybersecurity, data protection, and AML procedures. Any incidents or vulnerabilities must be reported immediately.

Background checks are carried out for staff with sensitive duties. Unauthorized devices or software are prohibited, and only approved equipment may be used to access company systems.

Incident Response and Breach Management

The Company maintains a structured incident response plan to address potential security events. The plan ensures: 1. Swift detection and containment. 2. Thorough investigation of causes and impacts. 3. Timely and transparent notifications to regulators, customers, and stakeholders, in line with legal obligations. 4. Restoration of systems to normal operation. 5. Incorporation of lessons learned into revised procedures.

Risk Management

Security risks are evaluated continuously, with full reviews conducted annually or following significant operational/technological changes. Independent penetration testing, audits, and certifications support the risk management process.

Risks are documented in a structured register, assessed for likelihood and impact, and mitigated with appropriate measures. Emerging threats such as fraud, cybercrime, and gaming system misuse are also addressed.

Compliance and Enforcement

Compliance with this Policy is mandatory. Employees breaching provisions may face disciplinary measures, while supplier breaches may lead to contract termination and potential regulatory reporting.

The Company recognizes that its gaming license depends on secure and responsible operations. Adherence to this Policy is therefore a condition of employment, partnership, and operation.

Review and Continuous Improvement

This Policy is reviewed annually, or sooner if required by regulatory, technological, or operational changes, or following incidents. Updates are approved by senior management and communicated to all stakeholders.

Information security is treated as an ongoing process of improvement. By investing in new solutions and awareness, the Company maintains a strong security posture.

Governance

The Board of Directors bears ultimate responsibility for the Company's information and systems security. Day-to-day oversight lies with the Chief Information Security Officer, who ensures sufficient resources, policies, and controls are in place.

Independent audits confirm compliance and provide assurance to regulators, stakeholders, and customers that DOUBLED B.V. operates with integrity and the highest security standards.

Approved by _____ **Roland Eduard Gertruda de Mei**
Director of DOUBLED B.V.

