

INFORMATION SECURITY & BETTING INTEGRITY POLICY

1. PURPOSE

This Policy sets out the principles, controls, and organisational measures adopted by Zozo Technology B.V., hereinafter referred to as the “Company” to ensure the security, integrity, availability, and reliability of its gaming systems and betting operations.

This Policy is established in accordance with the requirements of the National Ordinance for Games of Chance (LOK), applicable regulations, and supervisory guidance issued by the Curaçao Gaming Control Board, and applies to all systems, personnel, and third parties involved in the Company’s gaming activities.

2. SCOPE

This Policy applies to all betting systems, infrastructure, data, and operational processes supporting betting activities under JB and www.jb.com.

3. SECURITY OBJECTIVES AND ACCESS CONTROL

The Company ensures that:

- Bets are placed, processed, and settled accurately
- Betting systems remain available and resilient
- Betting data is protected against unauthorized access, alteration, or loss
- Betting outcomes are reliable, transparent, and auditable.

Access to gaming systems, databases, administrative interfaces, and critical infrastructure shall be restricted to authorised personnel only and granted on a least-privilege basis.

Appropriate authentication controls, including strong credential management and enhanced authentication for privileged access, shall be implemented.

Access rights shall be reviewed periodically and immediately revoked upon termination of employment or change of role.

4. GOVERNANCE AND ACCOUNTABILITY

The Company shall maintain a clear governance framework for information security and betting integrity.

A senior responsible individual shall be designated with overall accountability for system security and betting integrity compliance.

Roles and responsibilities relating to system administration, betting operations, payment handling, and compliance shall be clearly defined and subject to appropriate segregation of duties to prevent conflicts of interest and unauthorised activity.

5. INTEGRITY OF BETS

The Company shall implement effective measures to detect, prevent, and mitigate betting manipulation, fraud, collusion, insider betting, arbitrage abuse, and other activities that may compromise the integrity of betting operations.

Monitoring controls shall include automated and manual review of betting patterns, transactional behaviour, and account activity.

Controls are implemented to:

- Prevent unauthorized modification of bets or outcomes
- Ensure accuracy of odds, settlements, and balances
- Maintain traceability of betting transactions

The Company reserves the right to suspend, restrict, void, or withhold settlement of bets where there is reasonable suspicion of integrity breaches, in accordance with applicable terms and regulatory obligations.

6. AVAILABILITY & RESILIENCE

The Company maintains measures to ensure:

- System continuity and availability
- Redundancy and recovery capabilities
- Timely response to incidents or disruptions

7. CHANGE MANAGEMENT AND SYSTEM INTEGRITY

All material changes to gaming systems, betting logic, odds configuration, settlement mechanisms, or supporting infrastructure shall be subject to formal change management procedures.

Changes shall be documented, tested, approved, and logged prior to deployment to ensure continued system integrity and reliability.

8. INCIDENT MANAGEMENT AND REPORTING

The Company shall maintain documented procedures for the identification, investigation, and resolution of information security incidents and betting integrity breaches.

All incidents shall be recorded and investigated without undue delay, with corrective measures implemented as appropriate.

Where required by applicable law or regulatory instruction, material incidents shall be reported to the Curaçao Gaming Control Board or other competent authorities.

9. CONFIDENTIALITY & DATA PROTECTION

Measures are implemented to protect:

- Player personal data
- Betting and transaction data

- Access credentials and authentication mechanisms

Betting transactions, system logs, and relevant operational records shall be retained for a period sufficient to meet regulatory, legal, and audit requirements.

Records shall be protected against unauthorised alteration or deletion and shall remain accessible for inspection by authorised internal and external parties, including the Curaçao Gaming Control Board.

10. MONITORING & LOGGING

System activity is continuously monitored and logged in order to detect anomalies, unauthorised activity, or potential security incidents. Such monitoring and logging measures are also implemented to support internal investigations and audits, and to ensure that relevant records and evidence can be made available to regulatory authorities upon request, in accordance with applicable legal and regulatory requirements.

11. THIRD PART AND SUPPLIER CONTROLS

Where gaming systems or services are provided, hosted, or supported by third parties, the Company shall ensure that such providers maintain security and integrity standards consistent with this Policy and applicable regulatory requirements.

Third-party access to systems or data shall be subject to contractual safeguards, access controls, and ongoing oversight.

12. BACKUP, DISASTER RECOVERY AND BUSINESS CONTINUITY

The Company shall maintain appropriate backup, disaster recovery, and business continuity measures to ensure the availability and recoverability of critical systems and data.

Such measures shall be proportionate to the nature and scale of operations and reviewed periodically.

13. TRAINING

Personnel involved in betting operations, system administration, and compliance shall receive appropriate training on information security and betting integrity obligations.

Training shall be refreshed periodically and following material changes to systems or regulatory requirements.

14. CONTINUOUS IMPROVEMENT

Security and integrity controls are reviewed regularly in light of Risk assessments; Technological developments and Regulatory guidance.

Likewise this Policy shall be reviewed periodically and updated as necessary to reflect changes in regulatory requirements, operational risk, or system architecture.

VERSION	REASON	AUTHOR	DATE
1.0	Creation and Approval		