

Information Security Policy

Effective date: 30 July 2025

Last updated: 7 October 2025

1. Purpose

This policy defines how **JER-Team N.V.** protects player and company information in line with the Curaçao Gaming Authority (CGA) requirements and Article 5.3 of the *National Ordinance on Games of Chance (LOK)*. The goal is to ensure confidentiality, integrity, and availability of data and to prevent unauthorized access or misuse.

2. Scope

This policy applies to all employees, systems, and third-party providers involved in the gaming operations of **JER-Team N.V.** and covers all personal, financial, and operational data handled by the company.

3. Security Responsibilities

The company appoints an Information Security Officer (ISO) to oversee security controls and compliance. All employees must follow this policy and immediately report any security incidents. Third-party partners must meet equivalent security standards.

4. Data Protection

All player and company data is protected by encryption both in storage and during transfer. Access to sensitive data is limited to authorized personnel only, based on operational need. Multi-factor authentication is required for administrative accounts.

5. Network and Systems

Systems are protected by firewalls, antivirus tools, and monitoring software. Updates and security patches are applied promptly. Regular security reviews and vulnerability checks are conducted to ensure system safety and stability.

6. Incident Response

If a security incident or data breach occurs, the company investigates it immediately and reports significant cases to the CGA within 72 hours. Findings and corrective actions are documented for internal and regulatory review.

7. Backups and Continuity

Daily backups of critical systems are maintained in secure storage. Business continuity and recovery plans are in place to restore operations in case of system failure or data loss.

8. Staff Awareness

Employees receive basic training on data protection, secure system use, and how to recognize and report potential risks such as phishing or social engineering.

9. Record Keeping

Security records, logs, and incident reports are stored safely for at least five (5) years, as required by the CGA.

10. Policy Review

This policy is reviewed once a year or whenever operations or regulations change. Updates are approved by management and made available to the CGA and to players when applicable.

11. Contact

For information security or data protection inquiries, please contact:

Email: legal@roypins.com