

Information Security Policy – Pinbit N.V.

1. Policy Statement

Pinbit N.V. is committed to ensuring the **confidentiality, integrity, and availability** of all information systems, player data, and financial transactions.

This Information Security Policy (ISP) provides the framework for safeguarding data, mitigating cyber risks, and ensuring compliance with:

- **Curaçao GCA licensing requirements.**
- **GDPR and applicable data protection laws.**
- **Industry standards** (ISO 27001, PCI DSS, NIST).

2. Purpose

The purpose of this policy is to:

- Protect player information and company data against unauthorized access, loss, or misuse.
- Ensure compliance with **legal, regulatory, and contractual obligations.**
- Maintain secure and reliable gaming services for players worldwide.

3. Scope

This policy applies to:

- All employees, contractors, and third parties accessing company systems.
- All information systems, applications, networks, and databases.
- All forms of data (electronic, paper, verbal).

4. Core Principles

Pinbit N.V. adopts the following **information security principles**:

- **Confidentiality:** Data is accessible only to authorized individuals.
- **Integrity:** Data and systems must remain accurate and unaltered.
- **Availability:** Services and systems must be accessible when needed.
- **Accountability:** Every user is responsible for protecting data under their control.

5. Security Measures & Controls

5.1 Access Control

- Access granted strictly on a **need-to-know basis.**
- Multi-factor authentication (MFA) required for critical systems.
- Regular reviews of user access rights.

5.2 Data Protection

- All personal and financial data encrypted **in transit and at rest**.
- Data stored in secure, access-controlled environments.
- Backups performed daily and stored securely.

5.3 Network & Infrastructure Security

- Firewalls, intrusion detection/prevention systems (IDS/IPS) deployed.
- Regular patching and updates of operating systems and applications.
- Segregation of gaming systems, payment systems, and administrative networks.

5.4 Application Security

- Secure coding practices enforced for all software development.
- Regular vulnerability assessments and penetration testing.
- Critical vulnerabilities remediated within defined SLAs.

5.5 Payment Security

- Compliance with **PCI DSS** for handling payment card information.
- Use of regulated PSPs and secure payment gateways.
- Monitoring of payment anomalies (fraud detection systems).

5.6 Player Data Security

- Collection of **only necessary personal information**.
- Transparent privacy notices in line with GDPR.
- Players' right to request access, correction, or deletion of their data.

5.7 Incident Management

- All employees must immediately report **security incidents** (breaches, phishing, system failures).
- Dedicated **Incident Response Team (IRT)** investigates and mitigates incidents.
- Serious incidents reported to **regulator (GCA)** and affected players when legally required.

5.8 Business Continuity & Disaster Recovery

- Documented **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)**.
- Regular testing of failover and backup recovery systems.
- Objective: restore critical services within **24 hours**.

5.9 Training & Awareness

- Mandatory **security awareness training** for all employees.
- Specialized training for IT, compliance, and operations staff.
- Regular phishing simulations and security drills.

5.10 Third-Party Management

- Vendors, affiliates, and PSPs must meet **security and compliance standards**.
- Contracts include **confidentiality and data protection clauses**.
- Periodic vendor risk assessments performed.

6. Compliance & Monitoring

- Regular **internal audits** of security controls.
- Annual **independent security assessment** (penetration testing, ISO/PCI audits).
- Non-compliance may result in **disciplinary actions** or termination of contracts.

Director: Odin Trust B.V. represented by Christie Hansen

Date:

Signature: