

Information Security Policy

1. Objective

This policy defines the principles and procedures for maintaining the confidentiality, integrity, and availability of all information assets within the company. The organization is committed to protecting customer data, financial transactions, and internal systems against unauthorized access, disclosure, or damage.

2. Scope

This policy applies to all employees, contractors, and third parties who have access to our systems, networks, and data. It covers:

- Customer personal data
- Financial records
- Game and transaction systems
- IT infrastructure and cloud servers

3. Security Measures

- **Data Encryption:** All customer data and financial transactions are protected using SSL/TLS encryption.
- **Access Control:** System access is restricted to authorized personnel only, based on role and responsibility.
- **Passwords & Authentication:** Employees must use strong passwords and two-factor authentication (2FA).
- **Backups:** All critical data is backed up daily and stored securely in encrypted servers.

- **Firewalls & Monitoring:** Servers are protected by firewalls and 24/7 intrusion detection systems.

4. Data Protection

We follow the principles of GDPR and Curaçao data privacy regulations. Customer data may only be used for gaming, account verification, and compliance purposes.

Data shall not be sold or shared with third parties without legal basis or customer consent.

5. Incident Response

In case of a security breach, the IT Security Team must:

1. Immediately contain the incident.
2. Inform management and compliance officers.
3. Record details and analyze the root cause.
4. Notify affected users and regulators if required.

6. Employee Responsibilities

- Do not share passwords or login details.
- Lock systems when unattended.
- Report any suspicious emails or security breaches immediately.
- Avoid using personal devices for company operations without approval.

7. Policy Review

This policy is reviewed annually and whenever a significant change occurs in company systems or regulatory requirements.

Approved by:

IT & Compliance Department