

INFORMATION SECURITY POLICY

SUPER AWESOME GAMING ALLIANCE B.V.

T/A Power Win

Operating Under Curaçao LOK & Curaçao Gaming Authority (CGA)

1. Document Control

Document Title: Information Security Policy

Company: Super Awesome Gaming Alliance B.V.

Trading Name: Power Win

Jurisdiction: Curaçao

Regulatory Framework: LOK & CGA

Version: 1.0

Effective Date: February 2026

Review Date: Annual

Approved By: Board of Directors

This policy forms part of the Company's regulatory compliance framework under the Curaçao National Ordinance for Games of Chance (LOK).

2. Purpose

This Information Security Policy establishes the framework by which Super Awesome Gaming Alliance B.V. ("the Company") protects its information assets, player data, operational systems, financial transactions, and cryptocurrency infrastructure.

The objectives of this policy are to:

1. Protect the confidentiality of customer and corporate data.
2. Maintain the integrity of gaming systems and financial transactions.
3. Ensure availability and resilience of operational systems.
4. Meet regulatory requirements under LOK and CGA.
5. Mitigate cyber, fraud, and crypto-related risks.

This policy applies to all business activities conducted under the Power Win brand.

3. Scope

This policy applies to:

- All employees, directors, contractors, and consultants.
- Third-party service providers and outsourced partners.
- All IT infrastructure, servers, cloud environments, and applications.
- Customer personal data and KYC documentation.
- Financial and cryptocurrency transaction systems.
- Backup systems and disaster recovery infrastructure.

All individuals with access to Company systems must comply with this policy.

4. Governance & Responsibility

4.1 Senior Management Oversight

Ultimate responsibility for information security rests with the Board and Senior Management.

4.2 Designated Responsible Roles

The following roles support security governance:

- Chief Executive Officer (CEO)
- Compliance Officer
- Money Laundering Reporting Officer (MLRO)
- Data Protection Officer (DPO)
- IT / Security Manager

4.3 Responsibilities

Management shall ensure:

1. Appropriate security controls are implemented.
2. Risks are assessed and documented.
3. Incidents are properly managed and reported.
4. Regulatory obligations are fulfilled.

All staff must report suspected security breaches immediately.

5. Information Security Principles

The Company operates in accordance with the following principles:

5.1 Confidentiality

Information is accessible only to authorised individuals.

5.2 Integrity

Data is protected against unauthorised alteration.

5.3 Availability

Systems remain accessible and resilient.

5.4 Accountability

All critical actions are logged and traceable.

6. Risk Management Framework

The Company applies a documented risk-based approach consistent with LOK expectations.

6.1 Risk Categories

Security risk assessments consider:

- Cybersecurity threats
- Internal misuse
- Fraud and AML risks
- Cryptocurrency exposure
- Third-party risks
- Regulatory risks

6.2 Risk Classification

Risks are classified as:

- Low
- Medium
- High

Mitigation measures are applied proportionately.

Risk assessments are reviewed annually or following material operational changes.

7. Access Control & Authentication

Access to systems and data is strictly controlled.

7.1 Controls Implemented

- Role-Based Access Control (RBAC)
- Unique user IDs
- Strong password policies
- Multi-Factor Authentication (MFA)
- Least privilege principle
- Immediate access revocation upon termination

Administrative access is restricted and monitored.

8. Network & Infrastructure Security

The Company maintains a secure network architecture.

8.1 Controls Include:

- Firewalls
- Intrusion Detection / Prevention Systems
- Anti-malware software
- Secure configuration management
- Patch management processes
- DDoS protection
- Continuous system monitoring

Cloud infrastructure providers must meet recognised security standards.

9. Application & Platform Security

Gaming systems are developed and maintained securely.

9.1 Controls Include:

- Secure development lifecycle
- Code review procedures
- Vulnerability scanning
- Protection against common web threats
- Secure APIs
- Separation of development and production environments

Our third-party suppliers must meet equivalent security standards.

10. Data Protection & Encryption

Sensitive data is protected at all stages.

10.1 Protected Data Includes:

- Personal identification data
- KYC documentation
- Financial records
- Transaction logs
- Corporate confidential data

10.2 Security Controls

- Encryption in transit (SSL/TLS)
- Encryption at rest
- Secure key management
- Restricted access
- Data minimisation
- Secure deletion procedures

Data protection practices align with international standards, including GDPR-equivalent principles where applicable.

11. Cryptocurrency Security Controls

Where cryptocurrency is supported, enhanced safeguards apply.

11.1 Controls Include:

- Secure wallet management
- Separation of hot and cold storage
- Multi-signature authorisation
- Blockchain monitoring
- Sanctions screening of wallet addresses
- Protection against unauthorised withdrawals

Private keys are stored securely with restricted access controls.

12. Logging & Monitoring

All critical systems maintain audit logs.

12.1 Logged Events Include:

- User access and authentication
- Administrative changes
- Financial transactions
- System modifications
- Security alerts

Logs are protected from alteration and retained in accordance with regulatory requirements.

13. Incident Management & Breach Response

The Company maintains a documented incident response procedure.

13.1 Security Incidents Include:

- Data breaches
- Cyberattacks
- System compromise
- Fraud attempts
- Unauthorised access

13.2 Response Steps

1. Immediate containment
2. Investigation and assessment
3. Remediation
4. Documentation
5. Regulatory reporting where required

Affected customers will be notified when legally required.

14. Business Continuity & Disaster Recovery

The Company maintains resilience measures, including:

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Encrypted backups
- Redundant infrastructure
- Defined recovery objectives

Backup systems are tested periodically.

15. Third-Party Security Management

Third-party providers are subject to security due diligence.

15.1 Requirements Include:

- Security control assessment
- Confidentiality agreements
- Data protection compliance
- Ongoing monitoring

Contracts define security responsibilities and regulatory expectations.

16. Staff Training & Awareness

All staff receive mandatory security training.

Training includes:

- Cybersecurity awareness
- Data protection
- Secure handling of information
- Incident reporting
- Crypto risk awareness

Training is conducted at onboarding and periodically thereafter

17. Regulatory Compliance

The Company shall cooperate fully with the Curaçao Gaming Authority.

Material incidents impacting security or regulatory obligations shall be reported in accordance with LOK and CGA requirements.

18. Policy Review & Approval

This policy shall be reviewed:

- Annually
- Upon regulatory updates
- After significant incidents
- When operational changes occur