

Sculpture N.V

Information Security Policy

1. Purpose

This Information Security & Operational Integrity Policy establishes the framework for safeguarding the confidentiality, integrity, availability, and traceability of Sculpture N.V's systems and data.

The policy ensures the company delivers a safe, reliable, and compliant gaming environment and protects against external threats (e.g., hacking, fraud, phishing) and internal risks (e.g., data misuse, unauthorized access, operational failures).

This policy also defines controls required to comply with the regulatory requirements of the Curaçao Gaming Authority (CGA) and applicable data protection laws.

2. Scope

This policy applies to:

- all employees, contractors, vendors, and third-party partners with direct or indirect access to Sculpture N.V's systems;
- all data, systems, applications, gaming platforms, financial processing systems, and network resources owned, managed, or operated by Sculpture N.V or affiliated entities;
- all external service providers supporting platform operations;
- all digital infrastructure supporting gaming, player accounts, and financial transactions.

3. Information Security Governance & Risk Management

Sculpture N.V maintains a structured governance framework to ensure ongoing compliance, operational integrity, and risk oversight.

- A designated Information Security Officer (ISO) is responsible for policy implementation and regulatory liaison.
- Senior management receives periodic compliance and security risk reports.
- Information assets and operational risks are assessed regularly using a documented risk assessment framework.
- Controls are reviewed to ensure the gaming offering remains safe, reliable, and secure.

4. Data Hosting, Availability & Regulatory Access

To ensure operational resilience and regulatory oversight:

- Critical gaming systems and records are hosted in a Tier IV certified data center located and registered in Curaçao, or equivalent infrastructure approved by the CGA.

- Digital records relating to players, gaming activity, and financial transactions are maintained in secure systems and remain available to the CGA at all times upon request.
- The company maintains procedures enabling regulator access to systems, records, and audit trails in accordance with applicable laws.

5. Record Keeping & Audit Trail Controls

To ensure traceability and accountability:

- All player activity, gaming transactions, financial movements, system events, and administrative actions are logged.
- Logs are protected against alteration and retained in accordance with regulatory and legal requirements.
- Audit trails allow reconstruction of transactions and system activities.
- Access to logs is restricted and monitored.

6. Internal Information Security Guidelines

6.1 Acceptable Use

Company computing resources must be used for authorized business purposes. Personal use must remain minimal and must not compromise security.

6.2 Password Management & Authentication

- Strong, unique passwords are required.
- Multi-Factor Authentication (MFA) is mandatory for privileged and sensitive systems.
- Shared credentials are prohibited.

6.3 Access Control

- Access is granted based on least privilege and role necessity.
- Privileged access is restricted and logged.
- Access rights are reviewed regularly and revoked upon role change or termination.
- Development, testing, and production environments are segregated.

6.4 Data Classification & Handling

- Data is classified (Confidential, Internal, Public) and handled accordingly.
- Confidential data, including player and financial information, must be encrypted in transit and at rest.

6.5 Device & Endpoint Security

- Company-managed security software must be installed on all devices.
- Devices must be locked when unattended and regularly updated.

6.6 Security Awareness & Training

- Mandatory training at onboarding and annually thereafter.
- Periodic phishing simulations and awareness programs.

7. External Threat Protection & Platform Security

7.1 Phishing & Social Engineering

Communication systems are monitored for suspicious activity. Customers are educated on phishing risks via platform messaging and support channels.

7.2 Fraud & Transaction Monitoring

Automated fraud detection and behavioral monitoring systems identify suspicious gaming and financial activity.

7.3 Protection Against Unauthorized Access & Attacks

- Firewalls, IDS/IPS, and DDoS mitigation are deployed.
- Systems undergo regular penetration testing and vulnerability assessments.

7.4 Secure Software Development

- Code is reviewed, tested, and scanned for vulnerabilities before deployment.
- Third-party components are vetted and maintained.
- Security testing is integrated into the development lifecycle.

7.5 Software Installation Controls

Unauthorized software installation is prohibited. Administrative approval is required.

8. Protection of Player Funds & Credits

Technical safeguards ensure player balances and credits are protected against manipulation, loss, or unauthorized modification.

- Transaction integrity controls validate all balance adjustments.
- System controls prevent negative or inconsistent balances.
- Reconciliation processes verify financial accuracy.

9. Backup, Business Continuity & Disaster Recovery

To ensure safe and reliable operations:

- Data backups are performed regularly and stored securely in geographically separated locations.
- Backup integrity is tested periodically.
- Documented Business Continuity and Disaster Recovery (BC/DR) plans ensure restoration of critical systems within defined recovery time objectives.
- System restoration procedures are tested and maintained.

10. Incident Management & Reporting

10.1 Incident Classification

Incidents are classified and handled based on severity, including:

- security breaches,
- fraud or financial compromise,
- system failures,
- data loss or unauthorized access.

10.2 Response & Containment

All incidents must be reported immediately to the Information Security Officer. The incident response team will assess, contain, and remediate according to defined procedures.

10.3 Regulatory Reporting

Material security incidents must be reported to the Curaçao Gaming Authority within 24 hours of detection, with follow-up reporting as required.

Where required, affected users will be notified transparently.

11. Transaction Monitoring & Reporting Obligations

The company maintains systems and procedures to:

- record and monitor gambling transactions;
- detect irregular or suspicious activity;
- provide transaction records to regulators upon request;
- comply with applicable reporting obligations.

12. Regulatory Notifications & Amendments

Material changes to systems, controls, or operational structure affecting compliance must be reported to the CGA.

Semi-annual compliance updates and required amendment notifications are submitted by:

- 15 January, and
- 15 June.

13. Regulatory & Legal Compliance

Sculpture N.V complies with:

- Curaçao Gaming Authority regulatory requirements;
- applicable AML/CFT obligations;
- data protection laws including GDPR where applicable.

Regular internal and external audits support compliance assurance.

14. Roles & Responsibilities

- Management - responsible for policy enforcement, resourcing, and compliance oversight.
- Information Security Officer - responsible for security governance, incident reporting, and regulatory liaison.
- IT Security Team - responsible for monitoring systems, implementing safeguards, and ensuring compliance with technical controls.
- Staff - must comply with this policy, complete training, and report suspicious activity.
- Vendors & Third Parties - must comply with contractual security and compliance requirements.

15. Policy Review

This policy is reviewed annually or upon significant changes to:

- regulatory requirements,
- threat landscape,
- technology infrastructure,
- organizational structure.