



RIGT Data

RIGT DATA B.V.

INFORMATION SECURITY POLICY

1 Document Control

Date	Author	Approved By	Amendments made	Version number
12/09/2025	CEO	Director	Document Creation	1.0

2 Objectives

This Information Security Policy sets out the principles, responsibilities, controls, and procedures by which RIGT Data B.V. (the Company) will protect the confidentiality, integrity and availability of its information assets, including player data, transactional data, financial data, and software systems, to meet the requirements of the Curaçao Gaming Authority and applicable laws/regulations under the LOK, NOGC, NOIS, NORUT etc.

3 Scope

This policy applies to:

- All systems, networks, databases, applications, software, hardware, and data centres used in the development, delivery, maintenance, or support of gaming content, platforms, payment/settlement, player management or critical services.
- All employees, contractors, third-party service providers, suppliers, and other persons who have access to or process data on behalf of [Company].
- All environments (production, development, testing) and locations (on-premise, cloud, hybrid) where the company operates.

4 Legal and Regulatory Framework

In fulfilling this policy, the Company commits to:

- Complying with the LOK (National Ordinance on Games of Chance) and any policies, procedures, regulations, and guidelines of the CGA regarding information security.
- Ensuring that all software and equipment used comply with international information security standards and are tested by an independent qualified entity approved by the CGA.
- Protecting personal data of players and all transaction data in accordance with applicable laws (including the National Ordinance on the Protection of Personal Data) and CGA requirements.
- Ensuring service continuity (availability) and securing systems against interruptions, cyber threats, malware, intrusion, tampering, data breach.

5 Key Principles

Principle	Description
Confidentiality	Only authorised persons/processes may access sensitive data.
Integrity	Data and systems must be accurate, consistent, tamper-proof, and changes must be traceable.
Availability	Systems and services must be available to authorised users when required.
Accountability & Auditing	Actions affecting sensitive data or systems must be logged; audits and reviews conducted.
Least Privilege & Role Based Access	Access rights granted on needed basis; separation of duties.
Risk Management	Identify, assess, treat, monitor risks to information assets.
Incident Response	Defined process for detection, reporting, handling of security incidents.

6 Security Controls

6.1 Access Control

- Use authentication (multi-factor where appropriate) for all system access.
- Define roles and permissions; enforce least privilege.
- Periodic review of access rights.

6.2 Network & System Security

- Use network segmentation, secure subnets, firewalls.
- Encrypted communications (TLS etc) for data in transit.
- Encryption at rest for sensitive data.

6.3 Secure Development Lifecycle / Change Management

- Security requirements included from design phase.
- Code testing (including security testing, vulnerability scanning, penetration testing).
- Changes to production systems follow formal change management with testing, approval, rollback plans.

6.4 System & Software Maintenance

- Apply patches / security updates promptly.
- Use of supported software versions.
- Maintain inventory of hardware, software, games, platforms. CGA requires up-to-date inventory.

6.5 Monitoring, Logging & Audit

- Logging of user and system actions affecting critical data.
- Retain logs in a secure, immutable manner.
- Regular review of logs and periodic audits.

6.6 Data Protection & Privacy

- Classify data (public, internal, confidential, sensitive).
- Rules for handling, storage, access, transmission of personal data.
- Data retention and deletion policies consistent with legal obligations.

- Compliance with the National Ordinance on the Protection of Personal Data.

6.7 Physical Security

- Secure access controls to data centres / server rooms.
- Environment protection (power, climate, fire suppression).

7 Third-Party and Supplier Security

- All third parties (suppliers, contractors) that provide goods or services related to critical systems/software must adhere to at least equivalent information security standards.
- Contracts with third parties must include security, data protection, confidentiality clauses.
- Prior approval / due diligence required by CGA for critical service suppliers.

8 Incident Management

- Define process for identifying, classifying, reporting, mitigating security incidents.
- Incident reports to be submitted to the CGA within 24 hours after occurrence as required.
- Post-incident review and preventive actions.

9 Business Continuity & Disaster Recovery

- Maintain plans for continuity of critical services in case of outage, disaster or attack.
- Regular backups (secure, off-site or suitably protected) and testing of restore procedures.

10 Risk Assessment & Management

- Regular risk assessments (at least annually, or more frequently if major changes).
- Identification, analysis, mitigation, acceptance of risks.
- Maintain a risk register and track remediation.

11 Employee Awareness & Training

- Security training program for all employees, including specific training for those with elevated privileged access.
- Regular refresher training.
- Awareness of responsibilities re: confidentiality, phishing, social engineering etc.

12 Policy Governance & Review

- Information Security Officer (or equivalent) responsible for defining, owning, maintaining this policy.
- Regular review of the policy (e.g. annually) or after significant incidents or technology changes.
- Internal audits to check compliance.

13 Reporting & Compliance

- Maintain documentation proving compliance: test reports, audit reports, software and hardware test certifications, inventory etc.
- Submit policies, audited security documents and reports to CGA on request or within required timeframes.
- Cooperate with CGA during inspections, audits, investigations.