

TRIGONON GROUP N.V.

Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao • Company No. 142028 • www.goal365.bet

INFORMATION SECURITY POLICY

In accordance with the CGA Information Security Control Requirements — CIS Controls Implementation Group 1 (IG1)

Document Control

Document title	Information Security Policy
Version	1.0
Approved by	Board of Directors, Trigonon Group N.V.
Effective date	July 2026
Review date	Within 12 months after approval, and after any material change
Classification	Internal policy; may be provided to the Curaçao Gaming Authority (CGA) and approved auditors
Regulatory basis	Landsverordening op de Kansspelen (LOK); CGA Information Security Control Requirements for CGA Licensees (B2C and B2B), April 2026, or its successor

This Policy states the Company's control commitments. Supporting procedures, registers and evidence of control operation are maintained separately and are available to the CGA and approved auditors on request.

1. Purpose and Regulatory Basis

Trigonon Group N.V. (the “Company”), a company incorporated in Curaçao with registration number 142028 and registered address at Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao, operates the licensed online gaming website www.goal365.bet. The Company shall protect the confidentiality, integrity and availability of player information, player funds, gaming and financial transactions, game outcomes and supporting systems.

This Policy adopts the applicable Curaçao Gaming Authority (“CGA”) Information Security Control Requirements and CIS Controls Implementation Group 1 (“IG1”) as the Company's security baseline. Where a CGA requirement, licence condition or Curaçao law imposes a higher or more specific obligation, that obligation prevails.

2. Scope

This Policy applies to directors, employees, contractors, systems, devices, applications, networks, data and facilities used for the licensed operation. It also applies to outsourced services within the Company's regulatory responsibility, including platform, hosting, game, payment, sports-feed and security providers.

3. Governance and Proportional Implementation

- The Board of Directors retains overall accountability and designates a member of Senior Management to coordinate this Policy, report material risks and oversee remediation. A dedicated Information Security Officer is not appointed, consistent with the proportionate approach of the CIS IG1 baseline.

- Technical tasks may be performed by qualified employees, the platform provider, cloud provider or a managed security provider. Outsourcing does not remove the Company's regulatory accountability.
- The Company shall maintain a control-responsibility matrix showing, for each applicable control, the responsible party and supporting evidence.
- An information-security risk assessment shall be documented at least annually and after a material change or serious incident.
- Exceptions require documented risk justification, approval by the Policy Owner, compensating controls and an expiry or review date.

4. Security Controls

4.1 Assets and Software

- Maintain accurate inventories of hardware, network devices, software and gaming components, including owner, identifier, approval status, version and support status where applicable. Formal inventories are reviewed at least twice each year.
- Use a documented weekly process, automated or manual, to identify and address unauthorised devices; actions and approved exceptions shall be recorded.
- Check approved software support status at least monthly. Unsupported software shall be removed or covered by an approved exception and compensating controls.

4.2 Data Protection

- Classify data at least as Critical Gaming Data, Player Personal Data, Business Confidential or Public, and document permitted access, storage, transfer, retention and disposal.
- Maintain a current register of locations where sensitive data is stored, processed, transmitted or backed up; review it at least annually and after significant infrastructure change.
- Apply least privilege and encrypt sensitive data in transit and at rest using accepted industry-standard methods. Sensitive data on end-user devices must be encrypted.
- Define minimum and maximum retention periods. Gaming and transaction records shall be retained for the period required by the LOK, licence conditions and CGA instructions; secure disposal shall use appropriate deletion, cryptographic erasure, overwriting or physical destruction.
- Mask or anonymise player and other sensitive data used in development, testing or analytics unless use of identifiable data is authorised and protected.
- Maintain basic cryptographic-key controls covering authorised custody, storage, access, renewal or rotation, revocation and retirement.

4.3 Secure Configuration and Network Protection

- Use documented secure configurations. Disable unnecessary services and ports; disable, remove or secure default accounts and change default credentials before production use.
- Use host and network firewalls. Rule changes and exceptions must be authorised and recorded.
- Use encrypted administrative protocols such as SSH, SFTP and HTTPS. Insecure protocols shall be disabled unless risk-justified and approved.
- Maintain supported network firmware and software, review version status at least monthly and apply updates according to risk and vendor advice.

4.4 Accounts and Access

- Maintain an inventory of user, administrator and service accounts and formally review active accounts at least quarterly.
- Access requires recorded approval, is assigned by role and need-to-know, and is revoked immediately following termination, contract completion or relevant role change.
- Use separate administrator accounts for administrative activity and apply separation of duties where practicable.
- Require multi-factor authentication (MFA) for all externally accessible applications and portals, remote access, and administrative access to core gaming systems and infrastructure.
- Passwords must be unique and at least 8 characters when protected by MFA and at least 14 characters when MFA is not used. Default passwords are prohibited; approved password managers should be used where practicable.

4.5 Vulnerability and Patch Management

- Maintain a documented, risk-based vulnerability process covering asset discovery, scanning, prioritisation and time-bound remediation.
- Conduct vulnerability scans at least monthly, and more frequently where the risk to critical systems requires it.
- Apply operating-system, application, firmware and network patches at least monthly, subject to testing and documented risk-based exceptions. Record approvals, results and exceptions.

4.6 Logging and Monitoring

- Enable audit logging on applicable endpoints, servers, applications and security tools and send critical logs to central, access-restricted, tamper-resistant storage.
- Time-synchronise systems and protect log integrity by appropriate technical controls.
- Critical gaming logs shall include player activity, gameplay and betting transactions, game outcomes, jackpot and high-value events, deposits, withdrawals, bonuses and adjustments, administrative access and configuration changes.
- Document log-retention periods and conduct periodic anomaly reviews. Review the logging process at least annually and after significant system change.

4.7 Web, Email, Malware and Removable Media

- Use only supported and updated browsers and email clients, with automatic security updates where practicable.
- Use DNS or equivalent web filtering to block known malicious domains and monitor relevant anomalies.
- Protect supported endpoints and servers with centrally managed, automatically updated anti-malware controls and regular scanning, subject to documented compatibility exceptions.
- Disable automatic execution from removable media. Removable media requires authorisation and malware scanning before use.

4.8 Backup and Continuity

- Maintain a documented recovery process identifying critical systems and data, backup methods, security controls, recovery testing, recovery point objectives and recovery time objectives.
- Automate backups for sensitive or regulated data at least weekly and more frequently for high-volume gaming and financial transaction data where required to prevent unacceptable data loss.

- Protect backups with access controls and encryption and use offline, off-site or immutable storage where practicable. Periodically test restoration and record the result.
- Maintain and test business-continuity and disaster-recovery arrangements at least annually and after significant change, including appropriate failover or redundancy for mission-critical services.

4.9 Third Parties and Gaming Integrity

- Maintain a current inventory of providers, services, data exchanged, security responsibility, certification or audit status and contractual controls.
- Perform proportionate security due diligence before onboarding and periodic monitoring thereafter. Contracts shall include confidentiality, security, incident notification and a right to audit or request evidence.
- For CGA-regulated B2B game providers, verify required game, RNG and platform certifications at onboarding and at least annually. Certification lapses or withdrawals must be escalated, affected content suspended and the CGA notified where required.
- Authenticate and encrypt sports and gaming feeds, apply integrity validation, monitor availability and anomalies, and suspend affected markets or content when integrity cannot be assured.
- Where cloud or hosted services are used, document shared responsibilities and retain available assurance evidence such as recognised audit or certification reports.

4.10 Personnel and Physical Security

- Provide security awareness training on appointment and at least annually, including phishing, data handling, gaming fraud, social engineering and incident reporting. Provide role-based training for higher-risk roles where applicable.
- Apply confidentiality obligations and proportionate background screening for critical or sensitive roles, subject to applicable law. Recover assets and remove access on termination.
- Restrict physical access to offices, server rooms and other secure areas; maintain entry records where applicable and use appropriate surveillance, fire detection, environmental protection and power protection.
- Apply clean-desk and clear-screen practices and protect equipment used or stored away from Company premises.

5. Incident Response and CGA Reporting

- Maintain a documented incident-response procedure, a primary and backup incident coordinator, current internal and external contacts, escalation criteria, reporting templates and evidence-preservation requirements.
- Employees and providers must report suspected incidents immediately through the designated internal channel.
- The Company shall notify the CGA without undue delay and, in any event, within 24 hours of a security incident that compromises gaming integrity, affects player funds or personal data, or may impact regulatory reporting, system availability or game fairness, calculated in accordance with the LOK, licence conditions and current CGA instructions.
- Other authorities and affected persons shall be notified when required by applicable law. Material incidents shall receive a documented post-incident review and corrective actions.

6. CGA Data Access and Regulatory Cooperation

Critical information concerning players, gaming transactions and financial transactions shall remain accessible to the CGA through a server hosted in a Tier-IV certified data centre in Curaçao, in accordance with applicable CGA requirements. The Company shall provide requested information, permit authorised assessments and inspections, and cooperate with CGA oversight, including remote scanning and automated compliance verification where lawfully deployed by the CGA.

7. Compliance Assurance and Records

- Complete an annual self-assessment against all applicable CGA IG1 controls using the required form or current CGA instructions.
- Arrange independent third-party security audits where required for the online operation and maintain findings, remediation owners and target dates.
- Maintain an applicable-obligations register covering gaming, information security, privacy, AML/CFT/CPF and relevant contractual requirements.
- Retain sufficient evidence to demonstrate control operation, including inventories, approvals, reviews, scan and patch results, logs, backup tests, training, supplier checks, incidents and remediation.
- The Board of Directors or its delegate shall review material findings and overdue remediation.

8. Non-Compliance

Suspected breaches of this Policy must be reported promptly to Senior Management. The Company may take proportionate corrective or disciplinary action, up to and including termination of employment or contract. Regulatory non-compliance may result in CGA measures under the LOK and applicable licence conditions, including warnings, compliance directives, administrative financial sanctions and suspension of the licence.

9. Review and Approval

This Policy shall be reviewed at least annually and earlier following a material legal, regulatory, organizational, system or threat change, or a material incident — including upon publication of the final CGA Information Security Control Requirements following the public consultation. Amendments require approval under the Company's governance arrangements.

10. Reference Documents

- Landsverordening op de Kansspelen (LOK), as amended.
- Applicable CGA online gaming licence conditions and portal instructions.
- CGA Information Security Control Requirements for CGA Licensees (B2C and B2B), April 2026, or its successor.
- CIS Critical Security Controls, Implementation Group 1, as adopted by the CGA.
- Company policies published at www.goal365.bet: Terms of Service; KYC Policies, Privacy & Management of Personal Data; AML Policy; Fairness & RNG Testing Methods; Dispute Resolution Policy; Cookies Policy.

— END OF POLICY —