

Information Security Policy

1. Introduction

This Information Security Policy (hereinafter referred to as the "Policy") has been developed by Topxgo N.V. (hereinafter referred to as the "Company"), registered in Curaçao under number 165952, in strict compliance with the requirements of the Curaçao Gaming Control Board (CGA), including the National Ordinance on Games of Chance (LOK, P.B. 2024 no. 157), Supplier Licence Conditions (Art. 10(1)(a)), Supplier Licence (Art. 9(2)(c) and Art. 9(3)), Online Gaming Licence (Art. 7(1) and Art. 6(3)), NOOGH (Art. 5.10(6)), GDPR, as well as other applicable laws, regulations, recommendations, and studies.

The purpose of the Policy is to ensure the confidentiality, integrity, and availability of information assets on the platform, prevent data leaks, cyberattacks, and unauthorized access, minimize risks, and protect the data of players and the Company.

This Policy applies to all aspects of the Company's operational activities without exception, including, *inter alia*, gaming software, processing of players' personal data, financial transactions (including cryptocurrency operations in accordance with the Anti-Money Laundering and Know Your Customer Policy – AML & KYC), management systems, complaint handling procedures (in accordance with the Player Complaints Policy), and self-exclusion mechanisms (in accordance with the Self-Exclusion Policy), without any limitations in scope or nature.

It is equally binding for all employees, contractors, suppliers, and third parties with access to the Company's information, establishing strict obligations to maintain confidentiality and implement security measures within the framework of contractual relationships.

2. Definitions

- **Information Assets:** Player data, financial records, software, hardware, networks.
- **Information Security (IS):** Protection against threats to confidentiality, integrity, and availability (in accordance with ISO 27001).
- **IS Incident:** Data breach, DDoS attack, system or wallet compromise.
- **Personal Data:** Information about players (name, address, payment details, IP), and other information recognized as personal data in accordance with the Personal Data Processing Policy and GDPR.
- **KYC/AML:** Identification and anti-money laundering procedures integrated into IS.
- **Penetration Testing:** Vulnerability testing conducted by an accredited laboratory.
- **Encryption:** Data encryption.
- **Backups:** Data backup for recovery purposes.

3. Risk Identification and Assessment

The Company, in fulfillment of its obligations, is required to conduct risk identification and comprehensive assessment in strict accordance with the guidelines prescribed by the Curaçao Gaming Control Board (CGA), ISO 27001 standard, and analytical studies by ICGR

Research, taking into account a comprehensive analysis of potential threats and their consequences. The primary risks subject to priority consideration include:

- **Regulatory Risks:** Non-compliance with the requirements of Art. 10(1)(a) and Art. 9(2)(c), which may lead to license revocation (with a medium probability and high impact, requiring preventive measures).
- **Cyber Threats:** Distributed Denial of Service (DDoS) attacks, unauthorized intrusions (hacking), and leaks of confidential information (with high probability in the online gambling sector, including cryptocurrency transactions in accordance with the AML & KYC Policy).
- **Operational Risks:** Failures in software or hardware functionality, unauthorized access (considering risks associated with data storage in electronic wallets and verification procedures under the AML & KYC Policy).
- **Reputational Risks:** Loss of stakeholder trust due to security breaches, as reflected in Chainalysis reports for 2023–2025, where approximately 0.14% of cryptocurrency transactions were associated with illicit activities in 2024, with a steady downward trend in 2025.
- **Player Data Risks:** Breaches of confidentiality, non-compliance with data retention periods (not exceeding six years after account closure in accordance with the Privacy Policy and local legislation).

Risk assessments are conducted regularly using a risk matrix that integrates the calculation of probability multiplied by impact, supplemented by quantitative metrics (e.g., classification of risk as high if exceeding one incident per year; key performance indicator (KPI): less than 2% vulnerable systems). Scenarios identified as high-risk require immediate mitigation and elimination measures. Stress testing and external certification (e.g., by GLI laboratories) are performed as needed, depending on the level of identified risk, with a particular focus on GDPR-like regulations adapted to the Curaçao jurisdiction and their integration into complaint handling procedures in accordance with the Player Complaints Policy.

4. Security Measures

The Company's security measures are based on strict compliance with the requirements of the Curaçao Gaming Authority (CGA) and the ISO 27001 standard. The Company adheres to a zero-tolerance policy for violations, with measures adapted based on the level of risks, ensuring full compliance with licensing conditions and applicable legislation.

4.1. Dedicated Policy and Procedures

The Company maintains an up-to-date Policy and related procedures, including regular staff training as necessary (Supplier Licence Conditions, Art. 10(1)(a)).

The Policy is integrated with AML/KYC procedures for handling cryptocurrency transactions, ensuring comprehensive risk control.

4.2. System Inventory and Audit

The Company maintains an up-to-date register of hardware, software, and networks using CMDB tools for systematic asset accounting.

The Company conducts regular audits by an independent expert to verify system configurations as needed or upon significant changes (Supplier Licence, Art. 9(2)(c)); internal audits are performed based on risk levels, with results documented in accordance with CGA requirements.

4.3. Software Security Testing

The Company's gaming software and infrastructure undergo regular vulnerability testing by accredited laboratories based on risk levels (Online Gaming Licence, Art. 7(1)).

The Company conducts penetration testing, vulnerability scanning, and code reviews; the deployment of untested software is strictly prohibited in accordance with internal procedures.

4.4. Incident Reporting

Serious incidents (data breaches, DDoS attacks, system compromises) are reported to the CGA within 24 hours (NOOGH Art. 5.10(6); Supplier Licence, Art. 9(3)).

The Company applies an internal procedure for recording, analyzing, and resolving incidents; notifications to players and regulators are made in case of violations in accordance with the Privacy Policy, with escalation to ADR as per the Player Complaints Policy.

The Incident Response Team (IRT) operates 24/7, conducting simulations as needed to ensure prompt response.

4.5. Storage and Processing of Personal Data

Personal data is stored in encrypted form (AES-256) with backups as necessary (offsite storage, including servers in Germany in accordance with the Privacy Policy), with a retention period not exceeding 6 years after account closure or as required for compliance with applicable legislation (Online Gaming Licence, Art. 6(3)).

Data processing is based on consent, with minimization of data volume and ensuring players' rights (access, correction, deletion); international data transfers are conducted with adequate safeguards (in line with GDPR principles). Integration with AML & KYC procedures ensures verification and compliance with the Responsible Gaming Policy regarding self-exclusion data.

Unauthorized access to data is strictly prohibited; measures are integrated with the Privacy Policy for full compliance with regulations.

The Policy is reviewed and updated following significant system or regulatory changes.

4.6. Additional Measures

The Company employs firewalls, intrusion detection and prevention systems (IDS/IPS), multi-factor authentication (MFA), and access controls to protect infrastructure.

Staff undergo annual information security training as needed, with results documented in accordance with licensing obligations.

Physical security is ensured through restricted server access (CCTV, biometrics); supplier management includes assessments and audits based on risk levels, with a particular focus on compliance with AML & KYC for cryptocurrency service providers.

4.7. Information Classification and Management

Data is classified by levels (public, internal, confidential, restricted); appropriate protection measures are applied (e.g., encryption for restricted data).

Information management includes regular review of classification and destruction of outdated data based on risk levels, in accordance with internal procedures.

4.8. Business Continuity and Disaster Recovery

The Company has developed and implemented business continuity and disaster recovery plans to minimize downtime (e.g., backups, failover systems) as needed.

Plan testing is conducted regularly, with supplier assessments to ensure resilience based on risk levels, guaranteeing compliance with CGA licensing conditions and regulations.

5. Responsibility and Oversight

- **Chief Information Security Officer (CISO):** Responsible for implementation, monitoring, and reporting to the CGA, with mandatory documentation of all actions.
- **Company Management:** Approves the Policy, allocates resources, and bears personal responsibility for any violations that may lead to sanctions.
- **Employees:** Obligated to strictly comply; violations result in disciplinary measures, including termination or fines, in accordance with labor legislation.
- **Suppliers:** Ensure compliance with the Policy through contractual provisions; subject to mandatory audits and assessments.
- **Oversight:** Involves preparing reports for significant events, external reporting (including ISO audits) as needed, to ensure transparency and accountability.

6. Review and Update

The Policy is reviewed regularly as needed, following regulatory changes or incidents.

Latest version: August 17, 2025. Contact: security@top-x-go.com

Appendix A: Risk Matrix

Risk	Likelihood	Impact	Metric	Measures Taken
User data leakage	Low	Low	>1 breach/round	Compromised IRT, user identification
DDoS-attack	Medium	Low	>5% downtime	Monitored by monitoring department
Uncontrolled confidential leakage	High	Critical	>10% unauthorized access	Audited, investigated by audit department
Harassment of clients	Low	Medium	>20% retention loss for 6 months	Retention managed by PR department

Appendix B: Glossary of Extensions

- **ISO 27001:** International standard for information security management (2022 version).
- **IRT (Incident Response Team):** Incident Response Team.
- **MFA (Multi-Factor Authentication):** Multi-Factor Authentication.
- **IDS/IPS:** Intrusion Detection/Prevention Systems.