

TH Gambling N.V.

General Cyber & Information Security Policy

Document Control

Version	Date	Author	Description
1.0	24-09-2025	TH Gambling N.V.	Initial release
2.0	15-03-2026	TH Gambling N.V.	Full revision - LOK, GDPR, CGA 2026

1. Introduction

Information and information assets are vital resources for the Company (TH Gambling N.V., "the Company") and must be safeguarded by appropriate controls to lower the risks associated with their use.

This document demonstrates Management's commitment to a transparent security framework and its dedication to implementing and maintaining an Information Security Management System (ISMS) through continuous improvement.

The Company operates under a licence issued by the Curaçao Gaming Authority (CGA) pursuant to the National Ordinance on Games of Chance (LOK, in force 24 December 2024). This policy reflects the information security obligations under the LOK, CGA guidance, the Curaçao Personal Data Protection Ordinance (PDPO), and where applicable, the EU General Data Protection Regulation (GDPR).

2. Purpose and Objectives

The objective of this policy is to provide a framework for safeguarding the information and information assets of the Company, its players, clients, and suppliers against internal and external threats.

The three core principles underpinning this policy are:

- Confidentiality - information is accessible only to those authorised to access it.
- Integrity - information is accurate, complete, and protected from unauthorised alteration.
- Availability - information, systems, and services are accessible to authorised users when required.

The Company's information security objectives are to:

- Safeguard the information assets of the Company and protect its players' data and reputation.
- Comply with the LOK, CGA licence conditions, PDPO, GDPR, and PCI DSS.
- Build and maintain a security-aware culture through training and awareness.
- Detect, respond to, and recover from security incidents, including mandatory CGA regulatory reporting.
- Enable secure delivery of products and services in line with the Company's business strategy.

3. Scope of the ISMS

The ISMS covers the operations, processes, information assets, and personnel involved in delivering the Company's services. This policy applies to:

- All TH Gambling N.V. staff, including employees, contractors, and consultants.
- All information systems, infrastructure, and digital assets owned or managed by the Company.
- All third parties that process, store, or transmit data on the Company's behalf.

4. Policy Statements

The Company is certified under PCI DSS v4.0. ISO/IEC 27001, ISO/IEC 22301, and ISO/IEC 20000 are used as reference frameworks; the Company does not currently hold certifications under these standards.

Note: The Company uses ISO standards as guidance for enhancing internal processes only.

All personnel, contractors, and third-party service providers are required to comply with this policy and any supporting procedures. Non-compliance may result in disciplinary action, up to and including termination.

This policy has been reviewed and approved by Executive Management, communicated to all relevant stakeholders, and is reviewed annually.

5. Data Classification and Confidentiality

5.1 Classification Framework

All information assets are classified at the point of creation or receipt into one of four levels:

Level	Definition	Examples	Handling
Public	Approved for public release	Marketing, public T&Cs	No restrictions
Internal	General internal business information	Procedures, org charts	Internal use only
Confidential	Sensitive business or customer data	Player PII, KYC/AML records, financials	Need-to-know; encrypted at rest and in transit
Restricted	Highest sensitivity; severe impact if breached	CGA credentials, crypto keys, regulatory submissions	Named authorisation; full audit trail

5.2 Handling Requirements

Confidential and Restricted information must be encrypted at rest (AES-256) and in transit (TLS 1.3), accessed on a need-to-know basis only, shared with third parties only under a valid Data Processing Agreement, and securely disposed of when no longer required.

5.3 Player Data

Player personal data is classified as Confidential at minimum. Player account details, transaction records, KYC/AML documentation, and identity verification data are subject to the strongest protections under this policy and applicable data protection legislation.

6. Access Control

6.1 General Principles

Access to the Company's systems and data is governed by the principle of least privilege. Access rights are formally requested, approved, documented, and reviewed at least every six months and immediately on role change or termination. Shared accounts are prohibited. Multi-factor authentication (MFA) is mandatory for all remote access, privileged accounts, and systems containing Confidential or Restricted data.

6.2 User Account Lifecycle

Accounts are created only on receipt of a signed employment or contractor agreement and following completion of mandatory security training. Accounts are disabled on an individual's last working day and deleted within five working days. Contractor access is time-limited and reviewed monthly.

6.3 Privileged Access

Privileged accounts are granted only where strictly necessary. All privileged activity is logged and reviewed regularly. Privileged accounts must not be used for routine tasks; standard accounts must be maintained for day-to-day activities.

6.4 Remote Access

Remote access is permitted only via an approved VPN with MFA. All remote access sessions are logged. Direct remote desktop access to production servers requires prior written approval.

6.5 CGA Portal Access

In accordance with the CGA Portal Roles and Access requirements (January 2026), named account owners are designated for each CGA portal role. Credentials must not be shared. The Company accepts full accountability for all portal user actions. Portal access rights are reviewed every three months, and access is revoked within one working day of departure or role change.

7. Network Security

7.1 Network Access Controls

All network perimeters are protected by firewalls with rules reviewed every six months. Network traffic is logged and monitored. Business wireless networks are secured with WPA3 and segregated from guest networks. Unnecessary ports and services are disabled by default.

7.2 Network Segregation

The production gaming environment is isolated from development, staging, and office networks. Payment card processing systems are maintained in a dedicated PCI DSS cardholder data environment (CDE). Internet-facing systems are placed in a DMZ and cannot directly access internal databases. Third-party access is restricted to dedicated, monitored connection points.

7.3 Security of Network Services

All network services, whether internal or third-party, are operated in accordance with agreed security specifications. DDoS protection is implemented at the network perimeter with documented response procedures.

7.4 Infrastructure and Hosting

In accordance with Article 5.9 LOK, the Company maintains a physical server in a Tier IV certified data centre in Curaçao holding a digital register of critical player information. Player data is synchronised to this server at minimum weekly. A secondary backup is maintained locally in Curaçao. The CGA is granted direct audit access to this data at all times, and hosting contracts confirm this arrangement.

7.5 Encryption Standards

AES-256 encryption is applied to all data at rest in systems containing Confidential or Restricted data. TLS 1.3 (minimum TLS 1.2) is required for all data in transit over public networks. Weak or deprecated protocols (SSL, TLS 1.0/1.1, MD5, SHA-1) are prohibited. Cryptographic keys are rotated at least annually.

8. Security Awareness and Acceptable Use

8.1 Acceptable Use

Company systems are provided for legitimate business use. Personnel must not use Company systems for unlawful, offensive, or unauthorised purposes, install unapproved software, or attempt to circumvent security controls. Workstations must be locked when unattended. Suspected security incidents must be reported to the Security Officer immediately.

8.2 Email and Communications

Business email accounts must be used for all official communications. Confidential information must not be sent via unencrypted email. Suspicious or unsolicited emails must be reported to IT and must not be forwarded. Personal or unapproved messaging applications must not be used to share Company information.

8.3 Personal and Mobile Devices (BYOD)

BYOD access requires formal approval and deployment of a mobile device management (MDM) profile. Devices must be PIN or password protected, with full-disk encryption enabled. The Company reserves the right to remotely wipe Company data from approved BYOD devices upon loss, theft, or termination. Loss or theft of a device used to access Company systems must be reported to IT and the Security Officer immediately.

8.4 Social Media

Personnel must not share Confidential or Restricted information, player data, or details of security incidents or regulatory matters on social media or public platforms. All public communications relating to the Company must be approved by management.

8.5 Clean Desk and Clear Screen

Confidential documents and portable storage devices must not be left unattended in shared areas. Screens displaying sensitive information must not be visible to unauthorised individuals. Printed Confidential documents must be collected promptly and disposed of using secure shredding.

9. Personnel Security - Roles, Training, Rights and Duties

9.1 Roles and Responsibilities

Role	Key Responsibilities	Reports To
Executive Management	Overall accountability; policy approval; resource allocation	Board / shareholders
Security Officer	ISMS management; risk assessments; incident coordination; CGA cybersecurity documentation	Executive Management
LOK Compliance Officer	Monitor LOK compliance; liaise with CGA; coordinate licence activities	Executive Management; CGA
MLRO / AML Compliance Officer	AML/CFT programme; goAML FIU reporting; CDD/EDD oversight; AML training	Executive Management; FIU Curaçao
Responsible Gaming Officer	Player protection programme; annual RG compliance report to CGA	Executive Management; CGA
All Personnel	Policy compliance; incident reporting; mandatory training completion	Security Officer

9.2 Pre-employment Screening and Onboarding

Candidates for roles involving access to Confidential or Restricted data are subject to identity verification, right-to-work checks, and criminal background checks where legally permissible. Enhanced screening applies to key persons under the LOK. All new personnel must complete mandatory security awareness and AML training before system access is granted, and must sign acknowledgement of this policy.

9.3 Training Requirements

The minimum annual training requirements are:

- All personnel: information security awareness (phishing, password hygiene, incident reporting, data handling).
- All operational staff: AML/CFT awareness including CDD procedures and goAML reporting, as required by the CGA AML Policy (effective 10 April 2025).
- Key persons: regulatory updates covering LOK, CGA guidance, and GDPR/PDPO developments.
- IT and security personnel: role-specific technical training aligned with current threats.

Training completion is documented and records are retained for a minimum of three years, available to the CGA on request.

9.4 Rights and Duties of Personnel

Personnel have the right to clear guidance on their security obligations, to report concerns without retaliation, and to access the tools and training needed to fulfil their responsibilities. Personnel are duty-bound to comply with this policy, report incidents without delay, protect Company and player data, and complete mandatory training.

9.5 Disciplinary Process and Termination

Deliberate or negligent breach of this policy may result in disciplinary action up to and including termination. On departure, all access rights are revoked on the last working day, all Company devices and credentials returned, and CGA portal access revoked within one working day.

10. Incident Response and Reporting

10.1 Incident Classification

Severity	Description	Examples	CGA Reporting
Critical	Material breach, disruption or fraud	Hacking, data breach, fraud	Target 48 hours via CGA portal
High	Potential breach requiring urgent containment	Suspected unauthorised access	Report if confirmed
Medium	Security weakness not actively exploited	Vulnerability found, policy violation	Quarterly report
Low	Minor violation or anomaly	Lost access token	Internal log only

10.2 Response Procedure

On identification of a security incident: log the incident; contain and limit impact; escalate to the Security Officer (Critical and High) and Executive Management (Critical); investigate root cause; remediate; restore services; produce a post-incident report for all Critical and High incidents documenting root cause, corrective actions, and lessons learned.

10.3 CGA Regulatory Reporting

In accordance with Article 5.10 LOK, qualifying incidents must be reported to the CGA without delay via the mandatory CGA Incident Reporting Module (portal.cga.cw). Reportable incidents include security breaches affecting player data or game integrity, platform disruptions, fraud, and hacking. The target reporting time for Critical incidents is 48 hours. Reports must include a description, impact assessment, and corrective actions taken.

Note: The CGA Incident Reporting Module is the only mandatory reporting channel. Email or telephone reporting does not satisfy the Article 5.10 LOK obligation.

10.4 Data Breach Notification

For personal data breaches affecting EU-resident players, the relevant EU supervisory authority must be notified within 72 hours (GDPR). Affected individuals must be notified where the breach poses a high risk to their rights. Under the Curaçao PDPO, the Company will notify affected data subjects where material harm is likely. All personal data breaches are recorded and escalated to the Security Officer immediately.

11. Data Protection and Retention

11.1 Data Protection Principles

The Company processes personal data in accordance with the Curaçao PDPO and, for EU-resident players, the GDPR. Data is collected and processed only for specified, legitimate purposes; limited to what is necessary; kept accurate; retained only as long as required; and protected by appropriate technical and organisational measures (PDPO Article 13).

11.2 GDPR Compliance

To the extent the Company serves EU-resident players, GDPR applies extra-territorially. The Company maintains a Record of Processing Activities (Article 30), Data Processing Agreements with all third-party processors, data subject rights processes, and privacy by design on new processing activities. Breach notification to the relevant EU supervisory authority is within 72 hours.

11.3 Data Retention

Personal data and records are retained in accordance with the following minimum periods. Deletion or alteration of player records requires prior written CGA approval.

Record Type	Minimum Retention Period
Gaming and player account records	3 years from account closure or last transaction (LOK)
AML/CFT transaction records	5 years from transaction date or end of relationship (NORUT/LMOT)
KYC and identity verification records	5 years from account closure
Security incident records and training logs	3 years; available to CGA on request

12. Third-Party and Supplier Security

Due diligence is conducted on all third-party suppliers prior to engagement and on an ongoing basis. All third parties processing Confidential or Restricted Company data must have a formal Data Processing Agreement in place covering: scope and purpose of processing; security measures; incident notification obligations; audit rights; and data deletion on termination.

Third-party access to Company systems is granted on a least-privilege basis, time-limited, reviewed quarterly, and disabled after 30 days of inactivity. A register of all material third-party relationships is maintained by the Security Officer.

13. Physical and Environmental Security

Access to server rooms and data processing facilities is restricted to authorised personnel and is logged. The Company's primary player data server is located in a Tier IV certified data centre in Curaçao (LOK Article 5.9). Sensitive equipment and media must not be removed from premises without prior written authorisation. Physical documents containing Confidential or Restricted information are stored in locked cabinets and disposed of by secure shredding.

14. Business Continuity and Disaster Recovery

The Company maintains a Business Continuity Management programme aligned with ISO/IEC 22301 as a reference. Business Impact Analyses are conducted annually. Recovery procedures are documented and tested annually. Critical data backups are maintained in geographically separate locations, including the mandatory Curaçao secondary backup. Disruptions materially affecting the gambling offering are reported to the CGA under Article 5.10 LOK.

Policy Approval

This policy has been reviewed and approved by Management of TH Gambling N.V. and is effective from 15-03-2026. It supersedes all previous versions of the General Cyber & Information Security Policy.

Approved by	Date
Management, TH Gambling N.V.	15-03-2026