

TH Gambling N.V.

General Cyber & Information Security Policy

Effective Date: 24-09-2025

1. Introduction

- 1.1 Information and information assets are vital resources for the Company (TH Gambling N.V. “The Company”) and must be safeguarded by putting in place suitable controls to lower the risks associated with using them.
- 1.2 This document also demonstrates Management's commitment to create a transparent security policy and its dedication to putting Information Security Management System into place and keeping it up to date through continuous improvements.
- 1.3 To adhere to relevant laws, regulations, directives, and industry standards.

2. Purpose

The objective of this policy is to offer guidelines for safeguarding the information and information assets of the Company, as well as those of its clients and suppliers, against internal and external threats.

3. Scope of ISMS

The Information Security Management System (ISMS) covers the operations, processes, information assets, and people involved in delivering the company’s services and maintaining its systems.

4. Information Security Objectives

- 4.1 To safeguard the information and system assets of the Company, ensuring confidentiality, integrity, and availability of the company’s data, thereby protecting its reputation.
- 4.2 To adhere to relevant laws, regulations, directives, and industry standards.

4.3 To strengthen the security culture among employees, customers, and other stakeholders through ongoing cybersecurity and awareness initiatives.

4.4 To boost competitive advantage by securely enabling the development and delivery of new products and services.

4.5 To align the Company's security practices with its overall business strategy.

5. Policy Statements

5.1 The Company is compliant with the Payment Card Industry Data Security Standard (PCI DSS) which provides a robust framework for securing payment card data and associated environments.

5.2 In addition, the Company uses internationally recognized best practices, such as those from ISO/IEC 27001, ISO/IEC 22301, and ISO/IEC 20000, as references to strengthen its security posture, though it does not currently hold certifications under these frameworks.

Note: The company is not certified in these additional standards but uses them as guidance for enhancing internal processes.

5.3 All personnel, contractors, and third-party service providers are required to comply with this policy and any supporting procedures, standards, or regulatory requirements.

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

6. Applicability

This Policy applies to:

- All Th Gambling N.V. staff (employees, contractors, consultants).
- All information systems, infrastructure, and digital assets owned or managed by the company
- Any third-party entity that processes or manages data on behalf of the Company.

7. Reference Documents

- PCI DSS v4.0 (Certified Standard)
- ISO/IEC 27001:2022 - Information Security Management (reference only)
- ISO/IEC 22301:2019 - Business Continuity Management (reference only)
- ISO/IEC 20000:2018 - IT Service Management (reference only)
- Data Protection Act, 2012 (Act 843)
- Applicable Curaçao data protection and cybersecurity regulations
- International best practices and regulatory guidance where applicable