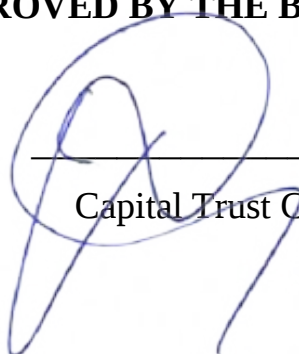


CAECUS N.V.

163779

INFORMATION SECURITY POLICY

APPROVED BY THE BOARD OF DIRECTORS



Capital Trust Corporation N.V.

1 Policy Statement

CAECUS N.V., a licensed provider of remote gaming services under the jurisdiction of Curaçao, acknowledges that information security and data protection are not only technical requirements but legal, regulatory, and ethical imperatives. The Company recognizes that its business model depends on the lawful and responsible management of sensitive information, including player financial records, personal data, and gaming activities.

Players, regulators, business partners, and the wider public must be confident that CAECUS N.V. operates in a manner that is secure, transparent, and accountable. Information security therefore represents a fundamental prerequisite for the sustainability of our operations, the protection of our license, and the preservation of the Company's reputation.

This Policy sets out the obligations and practices of CAECUS N.V. with respect to the protection of all information assets. It is specifically designed to ensure compliance with:

- the National Ordinance on Games of Chance (LOK), which establishes the licensing framework for Curaçao's gaming sector;
- the Regulations for the Combating of Money Laundering and the Financing of Terrorism (January 2025), which require robust monitoring, record-keeping, and reporting obligations for licensed operators;
- the Responsible Gaming Policy (February 2025), which ensures that vulnerable persons are protected and that gaming services are offered in a fair and transparent manner;
- the Curaçao Data Protection Act (CDPA), which regulates the lawful collection, storage, and processing of personal data within the jurisdiction; and
- where applicable, the European Union's General Data Protection Regulation (GDPR).

In addition to statutory requirements, this Policy is aligned with internationally recognized frameworks such as ISO/IEC 27001 and incorporates best practices from the regulated gaming industry. Together, these standards form a comprehensive basis for the Company's approach to safeguarding information, mitigating risks, and ensuring that the rights of players and stakeholders are fully respected.

2 Objectives and Scope

The overarching objective of this Policy is to establish a structured and enforceable framework that guarantees the confidentiality, integrity, and availability of all information assets managed by CAECUS N.V. In practical terms, this means:

- 1) Legal and Regulatory Compliance – ensuring that the Company fully complies with the LOK, AML/CFT obligations, Responsible Gaming standards, and applicable data protection laws (CDPA and GDPR).
- 2) Player Protection – safeguarding personal data, financial records, and gaming activities against unauthorized access, misuse, or manipulation, thereby protecting both player rights and the integrity of the gaming environment.
- 3) Operational Resilience – maintaining secure systems, networks, and business processes that can withstand technological failures, malicious attacks, or other forms of disruption, while ensuring continuous service availability.
- 4) Accountability and Transparency – providing assurance to the CGA, the FIU, and other relevant authorities that the Company maintains clear documentation, performs regular audits, and is fully accountable for the handling of data and information.
- 5) Continuous Improvement – embedding a culture in which security and compliance are not static requirements but dynamic processes that evolve in response to emerging risks, new technologies, and changes in regulatory frameworks.

This Policy applies to all directors, employees, contractors, consultants, and third-party suppliers engaged with CAECUS N.V. It covers all systems, infrastructure, and applications supporting the delivery of licensed gaming services, as well as all categories of data, whether physical or digital.

3 Governance Structure

The Board of Directors of CAECUS N.V. retains ultimate responsibility for ensuring that information security is maintained across the business.

The Compliance Officer is entrusted with the day-to-day responsibility for implementing this Policy and ensuring that all security controls align with legal and regulatory obligations. This includes oversight of AML/CFT requirements, Responsible Gaming safeguards, and data protection obligations.

The Compliance Officer provides regular reports to the Board, no less than once per year, detailing the effectiveness of controls, audit findings, and

recommendations for improvement. The Board remains accountable for approving resources, reviewing risks, and ensuring that corrective measures are enforced.

Independent internal and external audits will be carried out periodically to provide assurance of compliance. Their results are documented and made available to the CGA on request.

4 Risk Management Framework

CAECUS N.V. adopts a risk-based approach to information security, in line with both the AML/CFT Regulations (January 2025) and the principles of modern data protection law. This approach ensures that risks are systematically identified, documented, evaluated, and mitigated, with clear accountability at both operational and Board levels.

All identified risks are recorded in a formal Risk Register, maintained under the responsibility of the Compliance Officer and reviewed by the Board of Directors. Risks are assessed according to their likelihood of occurrence and the severity of their potential impact on players, business continuity, regulatory compliance, and reputation.

The risk management framework considers the following categories:

- 1) **Cybersecurity and Technical Threats** – including hacking, phishing, malware, denial-of-service attacks, unauthorized access to systems, and exploitation of software vulnerabilities.
- 2) **Operational and Continuity Risks** – arising from system failures, human error, inadequate supplier oversight, or natural disasters that could compromise the availability of services.
- 3) **Financial Crime Risks** – related to money laundering, terrorist financing, fraud, collusion, or match-fixing. These risks are directly connected to AML/CFT monitoring and unusual transaction reporting obligations.
- 4) **Responsible Gaming Risks** – linked to the potential harm caused to vulnerable players, excessive gambling behavior, or the failure of technical safeguards such as deposit limits, self-exclusion, or reality checks.
- 5) **Data Protection and Privacy Risks** – reflecting the Company's obligations under the Curaçao Data Protection Act (CDPA) and, where applicable, the EU General Data Protection Regulation (GDPR). Specific risks include unlawful collection or processing of personal data, failure to obtain proper consent, unauthorized cross-border data transfers, or insufficient safeguards leading to data breaches.

For each category, mitigation measures are defined and implemented. In the case of data protection, for example, this includes encryption, strict access controls, data minimization practices, and formal processes for responding to data subject rights requests.

The Risk Register is updated quarterly, with high or emerging risks escalated to the Board for immediate review. A comprehensive reassessment of all risks is conducted annually, and following any material change in technology, regulation, or business model. The Board approves the Company's overall risk appetite, ensuring that CAECUS N.V. does not knowingly assume risks that could compromise regulatory compliance, player protection, or the sustainability of its operations.

This risk management process is designed not only to meet the requirements of the CGA and the FIU but also to demonstrate compliance with the accountability principles embedded in both AML/CFT legislation and data protection frameworks such as the CDPA and GDPR. By aligning these obligations, CAECUS N.V. ensures that security and compliance are integrated into a single, coherent system of governance.

5 Information Security Principles

5.1 Infrastructure Protection

The Company employs multiple layers of defense to safeguard systems. Firewalls, intrusion detection, and DDoS protection are in place to secure the network. All gaming and payment connections are encrypted. Core systems are hosted in a Tier-IV certified data center in Curaçao, backed by disaster recovery solutions in separate locations.

5.2 Confidentiality

Confidentiality means that access to sensitive data is strictly limited to those with a legitimate business need. All player information, financial records, and compliance documents must be protected against unauthorized disclosure. This is achieved through encryption, secure authentication, and clearly defined role-based access rights.

5.3 Integrity

Integrity requires that data remains accurate, complete, and unaltered except by authorized processes. Systems are designed to detect any unauthorized modification, and every transaction is recorded in secure logs that cannot be tampered with. The accuracy of our gaming systems is verified through independent testing and certification.

5.4 Availability

Availability ensures that systems and data are accessible to authorized users when required. To achieve this, we employ redundancy in our infrastructure, maintain robust disaster recovery capabilities, and regularly test business continuity plans.

5.5 Accountability

Every employee and contractor is responsible for protecting information. Responsibilities are clearly documented in job descriptions, training programs, and disciplinary codes. Non-compliance with this Policy may lead to termination of employment or contract.

6 Monitoring and Auditing

System activity is monitored continuously to detect irregularities, suspicious transactions, or attempts to bypass security controls. Logs are stored in tamper-proof environments for at least five years.

Regular audits, both internal and external, verify compliance with this Policy, with AML/CFT laws, and with Responsible Gaming requirements. Audit results are shared with the Board and made available to the CGA.

7 Incident Response

CAECUS N.V. maintains a comprehensive Incident Response Plan to ensure that any event which threatens the confidentiality, integrity, or availability of information is dealt with in a timely, structured, and effective manner. The purpose of the plan is to limit damage, protect players and stakeholders, restore normal operations as quickly as possible, and demonstrate compliance with all legal and regulatory requirements.

7.1 Identification and Containment

All employees and contractors are obliged to report suspected security incidents immediately to the Compliance Officer. Incidents may include, but are not limited to: unauthorized access, attempted fraud, system outages, malware infections, data leaks, AML/CFT system failures, or breaches of Responsible Gaming controls. Upon detection, immediate measures are taken to contain the incident and prevent escalation.

7.2 Investigation and Root Cause Analysis

Each incident is logged and investigated to determine its scope, impact, and underlying cause. Investigations are documented in detail and reviewed by management. Findings are used to inform corrective and preventive measures.

7.3 Regulatory Reporting Obligations

The Company recognizes that certain incidents trigger mandatory notifications to regulatory authorities:

Curaçao Gaming Authority (CGA): Incidents that affect the integrity of licensed gaming operations or compromise player protection must be reported to the CGA within the timelines prescribed under the LOK and related directives.

Financial Intelligence Unit (FIU): Where an incident involves suspicious transactions, AML/CFT system failures, or indications of money laundering or terrorist financing, the FIU must be notified without delay, in line with the AML Regulations (January 2025).

Data Protection Authorities: In accordance with the Curaçao Data Protection Act (CDPA) and, where relevant, the EU General Data Protection Regulation (GDPR), personal data breaches that pose a risk to the rights and freedoms of individuals must be reported to the competent authority within the statutory timeframe (72 hours under GDPR).

7.4 Communication with Affected Players

Where an incident involves the compromise of player data or account balances, CAECUS N.V. will notify affected individuals promptly and in clear language. Such notifications will:

Describe the nature of the incident and the categories of data affected.

Outline the measures taken by the Company to contain the breach.

Provide advice to players on how they may protect themselves (for example, resetting passwords or monitoring financial accounts).

Explain the channels through which players can obtain further information.

This obligation applies under both the CDPA and GDPR, where notification to data subjects is required if the breach is likely to result in a high risk to their rights and freedoms.

7.5 Recovery and Business Continuity

Following containment and notification, priority is given to restoring systems and services to normal operation. Business continuity and disaster recovery procedures are activated where necessary to ensure uninterrupted access to essential gaming services and to protect player balances.

7.6 Post-Incident Review and Continuous Improvement

Each significant incident concludes with a formal review that identifies lessons learned and ensures that updated safeguards are implemented. Reports of incidents and their resolution are presented to the Board of Directors. The Risk Register is updated accordingly to reflect new or emerging threats.

8 Supplier and Third-Party Oversight

Third-party providers of critical services are subject to due diligence before engagement. Contracts must include obligations relating to AML/CFT compliance, Responsible Gaming requirements, and data security standards.

Suppliers are reviewed annually, with corrective action required for deficiencies. Persistent failure may result in contract termination and regulatory notification.

9 Personnel Responsibilities

All staff and contractors are personally responsible for complying with this Policy. They must attend regular training on cybersecurity, AML/CFT duties, and Responsible Gaming practices.

Employees in sensitive roles undergo pre-employment background checks. Breaches of this Policy may result in disciplinary action, dismissal, or regulatory reporting.

10 Compliance, Enforcement, and Review

This Policy is reviewed annually and whenever significant regulatory, operational, or technological changes occur. Updates are approved by the Board of Directors and communicated to all employees and relevant suppliers.

CAECUS N.V. commits to continuous improvement, ensuring that security practices evolve in line with emerging threats, innovations, and regulatory expectations.