

VELATUS N.V.

163778

INFORMATION SECURITY POLICY

Version 1.0/2025

Effective Date: September 29, 2025

Approved by: Board of Directors



Capital Trust Corporation N.V.

Policy Statement

VELATUS N.V., as a licensed operator within the jurisdiction of Curaçao, affirms that the preservation of information security and data integrity is central to its ability to lawfully deliver remote gaming services. The Company is entrusted with sensitive information, including financial transactions, personal records, and regulatory data, and acknowledges that its continued operation depends on the secure and transparent handling of these assets.

The purpose of this Policy is to articulate the commitments and responsibilities of VELATUS N.V. in relation to the safeguarding of information. It establishes obligations to comply with the **National Ordinance on Games of Chance (LOK)**, the **Regulations on the Combating of Money Laundering and Terrorist Financing (January 2025)**, the **Responsible Gaming Policy (February 2025)**, the **Curaçao Data Protection Act (CDPA)**, and, where applicable, the **General Data Protection Regulation (GDPR) of the European Union**. The Company also adheres to internationally recognized standards such as **ISO/IEC 27001**, ensuring that its internal practices reflect global expectations of the regulated gaming industry.

Objectives and Scope

This Policy has been established with the objective of creating a comprehensive, enforceable, and sustainable system for the protection of information assets. Its primary aim is to ensure that VELATUS N.V. not only complies with the letter of applicable laws and regulations, but also upholds the highest ethical and professional standards expected of a licensed operator in the global remote gaming industry. By embedding strong governance, technical safeguards, and accountability mechanisms into daily operations, the Company seeks to protect its license, its reputation, and the trust of its stakeholders.

The Policy is intended to deliver several core outcomes. First, it provides assurance of regulatory compliance, ensuring that VELATUS N.V. fully meets its obligations under the National Ordinance on Games of Chance (LOK), the AML/CFT Regulations, the Responsible Gaming Policy, and relevant data protection laws

(CDPA and GDPR). Second, it establishes a framework for player protection, guaranteeing that personal and financial data are treated with confidentiality and integrity, and that gaming services are delivered in a secure, transparent, and fair manner. Third, it reinforces operational resilience, ensuring that systems and processes can withstand external attacks, internal errors, and unforeseen disruptions without compromising service continuity or player balances.

The scope of this Policy is deliberately broad. It extends to all directors, employees, contractors, and consultants of VELATUS N.V., as well as to external service providers and suppliers engaged in delivering any aspect of the Company's licensed operations. It applies to all categories of data, including but not limited to: player personal records, payment transactions, gaming history, internal communications, business strategies, compliance documentation, and audit reports. It governs not only core production systems but also testing environments, backup facilities, cloud services, and disaster recovery sites.

Furthermore, the scope covers both technical infrastructure (servers, applications, networks, and endpoints) and organizational processes (onboarding procedures, customer due diligence, staff training, supplier vetting, and reporting mechanisms). In doing so, it creates a unified and consistent security posture across the entire business ecosystem. The Policy also applies to any activity that involves the processing, transfer, or storage of information, regardless of whether such activity is performed directly by the Company or delegated to a third party.

By defining objectives in this way and extending the scope across all operational layers, VELATUS N.V. ensures that information security is not confined to the IT department but is instead treated as an organization-wide responsibility that is critical to lawful, ethical, and sustainable gaming operations.

Governance

The Board of Directors of VELATUS N.V. retains overall accountability for information security. Oversight of the implementation of this Policy rests with the Compliance Officer, who is charged with ensuring that appropriate measures are in place to align security practices with statutory and regulatory

obligations. The Compliance Officer is required to provide at least annual reports to the Board regarding the adequacy of security controls, audit findings, and recommended improvements.

The Company also recognizes the necessity of independent assurance. For this reason, both internal and external audits shall be conducted periodically, with results recorded and shared with the Curaçao Gaming Authority (CGA) when required.

Risk Management Framework

VELATUS N.V. adopts a structured, risk-based methodology to the management of information security. Risks are identified, assessed, and documented in a formal register, which is maintained under the authority of the Compliance Officer and subject to Board review. Each risk is evaluated according to its probability and potential impact on the Company's ability to operate lawfully and responsibly.

The categories of risk addressed include:

- threats to cybersecurity such as malware, phishing, and network intrusion;
- operational vulnerabilities arising from system failures, supplier dependencies, or natural disasters;
- risks relating to money laundering, terrorist financing, fraud, or collusion;
- issues connected with Responsible Gaming, including the failure of systems to protect vulnerable players; and
- privacy and data protection risks as defined by the CDPA and GDPR, including data breaches and unlawful processing.

The register is updated on a quarterly basis and fully reassessed each year. High-risk issues must be escalated to the Board immediately, and mitigation strategies shall be approved at the highest level.

Information Security Principles

VELATUS N.V. is guided by a set of fundamental principles in its approach to security:

- **Confidentiality** is ensured by restricting access to sensitive information to those who have a clear business need.

- **Integrity** is maintained through systems that prevent unauthorized alteration and preserve accuracy.
- **Availability** is guaranteed by the use of redundant infrastructure, tested disaster recovery procedures, and continuity planning.
- **Accountability** is embedded in every role within the Company, with responsibilities for security clearly defined.

Infrastructure is protected by layered defenses, including firewalls, intrusion detection, and DDoS mitigation. All core systems are hosted in Curaçao within a Tier-IV certified data center, supported by geographically distinct recovery facilities.

Monitoring and Auditing

All systems are subject to continuous monitoring to detect irregular or suspicious activity. Security logs are retained for no less than five years and safeguarded against tampering. The Company conducts regular audits, internal and external, to confirm adherence to this Policy, AML/CFT requirements, Responsible Gaming obligations, and data protection laws.

Incident Response

VELATUS N.V. maintains a comprehensive plan for responding to incidents that threaten the confidentiality, integrity, or availability of its information systems.

All incidents must be reported immediately, investigated thoroughly, and documented in detail. Where required by law, the Company shall notify:

- the Curaçao Gaming Authority (CGA) of any issue affecting licensed operations;
- the Financial Intelligence Unit (FIU) in the case of AML/CFT failures or suspicious transactions; and
- data protection authorities under the CDPA or GDPR in the case of breaches affecting personal data.

Players whose accounts or data are compromised shall also be informed in clear and timely communications. Once incidents are contained, recovery measures are enacted to restore normal

operations, and lessons learned are incorporated into revised procedures.

Supplier and Third-Party Oversight

Given the reliance on third-party service providers, VELATUS N.V. imposes strict requirements on its suppliers. Due diligence is carried out prior to engagement, and contractual terms obligate suppliers to comply with the same standards of information security, AML/CFT controls, and Responsible Gaming requirements as the Company itself. Suppliers are reviewed annually, and deficiencies may result in corrective measures or termination of contracts.

Personnel Responsibilities

Every employee, director, and contractor of VELATUS N.V. is required to comply with this Policy. Mandatory training is provided covering cybersecurity awareness, AML/CFT obligations, and Responsible Gaming practices. Staff in sensitive positions undergo background checks prior to appointment. Breaches of this Policy may result in disciplinary action, dismissal, or notification to regulatory authorities.

Compliance and Review

This Policy is binding across the Company. It shall be reviewed at least annually and whenever significant changes occur in the regulatory, operational, or technological environment. Updates must be approved by the Board of Directors and communicated to all relevant personnel and partners.

VELATUS N.V. is committed to continuous improvement in its security posture, recognizing that information security is an evolving discipline requiring vigilance, investment, and proactive governance.