

INFORMATION SECURITY POLICY

CARLETTA N.V.

Registration No. 142346

Registered address: Dr. Henri Fergusonweg 1, Curaçao

License No. OGL/2024/580/0570

Signed on behalf of Carletta N.V.:

Name: (SMES) Solution for Management and Employment Support N.V.

Position: Director

Date: 25.09.2025



1. Purpose and Scope

This Information Security Policy defines the purpose, direction, principles and basic rules for managing information security at Carletta N.V. It applies to all licensed platforms, operational data storage systems, and employees, contractors, and relevant external parties. The policy is part of the overall Information Security Management System (ISMS) that ensures planning, implementation, maintenance, review, and improvement of security in line with the company's objectives.

2. Objectives

- Protect player personal data, KYC/AML records, and financial transactions in line with CGA and local data protection law.
- Ensure security of iGaming processes, RNG outcomes, and payment operations.
- Guarantee resilience and availability of the system hosted on AWS EU and Curaçao Tier IV storage.
- Detect, mitigate, and respond to incidents in real time.
- Provide audit-friendly storage accessible to CGA.

3. Roles and Responsibilities

Responsibility for compliance with this policy rests with specific roles within the company. The IT and Security Team implements encryption protocols such as AES-256, TLS 1.3, and IPSEC, in addition to patching and monitoring systems. All employees and contractors are obliged to comply with the security rules and report incidents, while third-party providers, such as payment and KYC services, are bound by outsourcing and data protection agreements.

4. Access Control

Access rights are formally approved, regularly reviewed, and revoked immediately when no longer required. Multi-factor authentication is mandatory for privileged accounts. Role-based access controls are applied, and sensitive data is transmitted over encrypted VPN channels restricted to whitelisted endpoints.

5. Data Protection

The company protects sensitive information by applying AES-256 disk-level encryption to the Ceph cluster and enforcing TLS 1.3 with RSA-2048 or ECDHE for all data transfers. Depending on the dataset, additional obfuscation methods such as SHA-256 or HMAC hashing, deterministic encryption (AES-SIV), and format-preserving encryption (FPE) are used. Data retention rules mandate that player profiles, KYC, AML, and management transactions are kept for five years since the last bet, while deposit, withdrawal, and refund transactions are maintained for five years as well. All backups are stored in encrypted form at the Curaçao Tier IV data center and replicated to ensure continuity.

6. System and Network Security

Hybrid hosting in AWS EU and a Tier IV data center in Curaçao ensures resilience and continuity. Networks are protected with TLS 1.3, IPSEC VPNs, endpoint allow-lists, WAF, and DDoS protection. Segregation of environments and regular vulnerability scans and penetration testing are in place.

7. Transaction and Payment Security

All PSP integrations are PCI DSS compliant. Payment operations are processed in segregated accounts to guarantee payout availability. Financial data is logged and stored in secure systems with full audit trails.

8. Monitoring and Logging

Audit logs include system changes, administrative access, and financial transactions. Logs are retained for at least five years in compliance with CGA requirements. SIEM tools provide real-time alerts, and anomalies are investigated daily.

9. Business Continuity and DR

Redundant systems across multiple nodes ensure a 99.9995% SLA. Recovery Time Objective (RTO) is four hours, and Recovery Point Objective (RPO) is fifteen minutes for critical systems. Disaster recovery plans are tested annually.

11. Training and Awareness

Training and awareness programs are mandatory for all staff, beginning with onboarding sessions in information security and continuing with quarterly refreshers, including phishing awareness. Technical staff undergo specialized security training. Awareness campaigns ensure that all staff understand their security responsibilities.

12. Third-Party and Supplier Security

All third parties must demonstrate compliance with annual reviews of vendor security practices are conducted.