

INFORMATION SECURITY & DATA PROTECTION POLICY

Approved by the Board of Directors

Company name	ASPRO N.V.
Version	2025/V.1
Authorized Signatory	 (SMES) Solutions for Management and Employment Support N.V.
Date of Approval	September 25, 2025

This Policy is subject to copyright law and any reproduction of all or part of the contents in any form is prohibited.

1 INTRODUCTION AND PURPOSE

ASPRO N.V. conducts licensed remote gaming operations under Curaçao law. Protecting information assets, gaming systems, and player data is essential for operational integrity, regulatory compliance, and the safeguarding of vulnerable persons.

This Policy establishes the security framework necessary to ensure:

- Confidentiality – safeguarding player and company information against unauthorized disclosure.
- Integrity – preventing unauthorized alteration or manipulation of systems, data, and gaming outcomes.
- Availability – ensuring licensed services remain resilient and accessible to players and regulators.
- Compliance – adherence to the National Ordinance on Games of Chance (LOK), AML/CFT regulations, Responsible Gaming requirements, and international standards (e.g., ISO/IEC 27001).

The Policy is binding on all employees, contractors, partners, and suppliers, and will be subject to regular audit and review to ensure that it continues to reflect the evolving regulatory and technological environment in which the Company operates.

2 SCOPE

This Policy applies to all information assets owned, leased, or otherwise managed by ASPRO N.V. It encompasses every employee, consultant, contractor, and third-party supplier who has access to Company systems or data.

The scope includes, but is not limited to:

- All production systems supporting gaming operations, payment processing, and customer services.
- Corporate networks, internal communication tools, cloud platforms, and backup environments.
- Data in any form, whether physical (e.g., printed reports), electronic (e.g., databases, transaction logs), or visual (e.g., CCTV).
- Player records, financial transactions, corporate communications, compliance reports, and operational documentation.
- By explicitly including suppliers who provide Critical Services or Goods (as defined in Article 1.1(g) of the LOK), this Policy extends the obligation of compliance beyond our internal environment to every partner that has the potential to impact the security and continuity of our licensed operations.

3 GOVERNANCE AND ACCOUNTABILITY

The Board of Directors has ultimate responsibility for ensuring that information security is embedded in the Company's strategy. The Board delegates operational oversight to the Chief Information Security Officer (CISO), who is responsible for implementing this Policy, allocating resources, and ensuring that appropriate risk management processes are in place.

The Compliance Officer plays a parallel role in ensuring that information security controls align with AML/CFT obligations, sanctions regulations, and Responsible Gaming requirements. This dual structure ensures that security is not viewed narrowly as an IT matter but as a holistic compliance function.

Independent assurance is obtained through both internal audit and external third-party assessments. These audits are conducted at least annually, with additional targeted reviews following major incidents, technological upgrades, or changes in regulatory expectations. Audit findings are reported to the Board and shared with the CGA upon request, demonstrating our commitment to transparency and accountability.

4 GOVERNANCE AND ACCOUNTABILITY

Information security risk management is an ongoing process rather than a one-time exercise. The Company maintains a formal Risk Register in which every identified threat is recorded, assessed, and assigned an owner. Each risk is evaluated in terms of its likelihood and potential impact, using a structured methodology that aligns with both ISO/IEC 27005 and the risk-based approach prescribed by the AML Regulations of January 2025.

Risks considered include, but are not limited to:

- Cybersecurity threats such as hacking, phishing, DDoS attacks, or ransomware.
- Fraud and collusion, including match-fixing or manipulation of odds.
- Financial crime risks associated with money laundering or terrorist financing.
- Player-related risks, including the misuse of accounts by vulnerable or underage persons.
- Operational risks arising from new technologies such as cryptocurrencies, e-wallets, AI-based betting tools, or cloud infrastructure.

The Risk Register is reviewed quarterly and formally updated at least once a year. Where risks are rated as high or critical, the Board must be notified and appropriate mitigation measures approved.

5 Information Security Principles

5.1 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.

5.2 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.

5.3 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.

5.4 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 Network and Infrastructure Protection

The Company adopts a layered defense model to secure its IT environment. Firewalls, intrusion prevention systems, and DDoS mitigation services protect our perimeter. All connections to gaming platforms and payment systems use end-to-end encryption based on industry best practices (TLS 1.3 or higher).

Critical systems are hosted in Curaçao within a Tier-IV certified data center, as required by Article 5.9 of the LOK. Backup facilities exist in geographically separate locations, ensuring continuity even in the event of natural disasters or large-scale system failures.

Regular vulnerability scans and penetration tests are conducted, both internally and by accredited external firms. Findings are tracked until remediation is confirmed.

7 Access Control

Access rights are governed by the principle of least privilege. Users receive only the permissions required to perform their duties. Multi-factor authentication is mandatory for all privileged accounts. Session timeouts and monitoring prevent unauthorized persistence of access.

Access rights are reviewed monthly, and immediately revoked when an employee leaves the Company or changes roles. Any attempt at unauthorized access triggers automatic alerts to the security operations center.

8 Data Protection and Privacy

The Company processes large volumes of sensitive data, including personal information, financial records, and behavioral profiles. Data protection is therefore at the heart of this Policy.

All personal data is encrypted at rest and in transit. Data retention follows the AML Regulations, requiring records to be kept for at least five years. Players are informed about how their data is processed through a clear privacy notice, and they may exercise data subject rights in accordance with applicable law.

Particular care is taken to segregate player balances and winnings from operational funds. This segregation ensures that even in the event of insolvency or system compromise, player assets remain protected.

9 Monitoring and Auditing

Security and compliance monitoring are continuous processes. Centralized logging systems collect data from all servers, applications, and network devices. These logs are reviewed in real time to identify suspicious activity, including unusual login patterns, irregular financial transactions, or attempts to bypass responsible gaming controls.

Audit trails are immutable and retained for at least five years. Both internal and external auditors review these records to ensure compliance with CGA directives. Where deficiencies are identified, corrective action plans are developed and tracked through completion.

10 Incident Response and Breach Management

The Company maintains a comprehensive Incident Response Plan that covers cybersecurity breaches, fraud attempts, system outages, and other events that could compromise information security.

When an incident occurs, the priority is to contain the threat, protect player balances, and restore normal operations as quickly as possible. A structured process ensures that incidents are logged, investigated, and remediated.

Significant incidents are reported to the CGA and, where applicable, to the FIU or data protection authorities. Players are notified if their data has been compromised, in line with regulatory requirements. Lessons learned from incidents are incorporated into revised policies and procedures.

11 Supplier and Third-Party Oversight

Suppliers play a critical role in the gaming ecosystem, providing hosting, payment processing, and other essential services. To manage third-party risks, the Company requires suppliers to undergo due diligence prior to engagement.

Contracts with suppliers must include clauses obligating them to comply with AML/CFT, Responsible Gaming, and information security standards. Regular assessments verify that these obligations are met. Where suppliers fail to maintain required standards, the Company may terminate the relationship and report the issue to the regulator.

12 Employee Responsibilities and Training

Every employee is responsible for safeguarding the Company's information assets. To prepare staff for this responsibility, the Company provides mandatory training on cybersecurity, AML/CFT requirements, and Responsible Gaming obligations. Training is repeated annually and updated when regulations or technologies change.

Employees in sensitive positions undergo pre-employment screening, including background and integrity checks. Breaches of this Policy may result in disciplinary action up to dismissal.

13 Compliance, Enforcement, and Review

This Policy is binding on all personnel. Failure to comply may result in disciplinary measures, contract termination, or regulatory reporting.

The Policy is reviewed annually, and more frequently if significant changes occur in law, regulation, technology, or risk environment. Updates are approved by the Board of Directors and communicated to all employees and suppliers.

Continuous improvement is a core principle: information security is treated as a dynamic process requiring ongoing investment, adaptation, and cultural reinforcement.