

Information Security Policy

Version 1.0

Effective Date: September 2025

Table of Contents

1. Introduction.....	3
2. Scope and Applicability.....	4
2.1. Purpose of the Policy.....	4
2.1.1. Strategic Security Objectives.....	4-5
2.2. Scope of Information.....	5-6
2.3. Scope of Information Systems.....	6
2.4. Third- Party and Outsourced Services.....	6-7
2.5. Users Covered by this Policy.....	7
3. Individual Responsibilities.....	7
3.1. All Employees, Contractors and Partners.....	7-8
3.2. System Users and Data Handlers.....	8
3.5. Data Protection Officer (DPO).....	8-9
4. Compliance.....	9
4.1. Awareness and Training	9-10
4.2. Monitoring and Enforcement.....	10
5. Specific Security Objectives.....	10
6. Oversight and Governance.....	11
7. Other Policies.....	11

1. Introduction

INNOVEX B.V. is a limited liability company incorporated under the laws of Curaçao, registered under company number 165563, with its registered office located at Zuikertuintjeweg Z/N, Curacao. The Company is engaged in the organization, marketing, promotion, management, support, operation, and facilitation of all types of games of chance, hazard, and skill. This includes the development and launch of gaming products such as interactive casinos, bingo, lottery, poker, and other interactive games, including sports betting. Additionally, the Company may buy, sell, acquire, or provide products and licenses related to games of chance and skill. Hereinafter, the company may be referred to as “the Company.”

This Information Security Policy (hereinafter referred to as the “**Policy**”) defines the core principles, responsibilities, and security measures that the Company has implemented to protect its data, systems, and services. It is designed to ensure the confidentiality, integrity, and availability of the Company’s critical information assets, while minimizing the risks associated with unauthorized access, data breaches, and service disruptions. The Company is committed to maintaining robust information security practices, which include safeguarding sensitive and confidential data from unauthorized access or disclosure, ensuring the accuracy and reliability of all information and systems, and ensuring that critical systems and services remain available and operational.

This Policy applies to all employees, contractors, vendors, and any third parties who interact with or have access to the Company’s information systems. It serves as the foundation for all security-related activities within the organization. The Policy establishes a comprehensive framework to safeguard the Company’s information assets, manage information security risks, and ensure adherence to relevant international standards and regulatory requirements, including but not limited to:

- ISO/IEC 27001:2022 – Information Security Management Systems (ISMS);
- ISO/IEC 27002:2022 – Code of Practice for Information Security Controls;
- General Data Protection Regulation (EU) 2016/679 (GDPR);
- Curaçao eGaming regulations, including applicable Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance obligations;
- Other applicable AML, Counter-Terrorist Financing (CTF), and responsible gaming laws and guidelines.

2. Scope and Applicability

2.1. Purpose of the Policy

2.1.1. The Information Security Policy is designed to ensure the protection of the Company's information assets in a manner that aligns with internationally recognized best practices, applicable legislation, and the expectations of regulators, customers, and business partners. This Policy outlines the security measures necessary to maintain the confidentiality, integrity, and availability of the Company's data, systems, and services.

The Policy is built on three fundamental security principles. First, confidentiality ensures that access to sensitive information is strictly controlled and granted only to authorized individuals and systems, protecting confidential data from unauthorized disclosure. Second, integrity guarantees that all information assets remain accurate, reliable, and safeguarded against unauthorized or accidental modifications. Systems and networks are to function as intended, without compromise. Lastly, availability ensures that information and services are accessible and operational when needed, supporting the uninterrupted operation of business processes, customer interactions, and compliance with regulatory requirements.

In support of these principles, the Company is committed to achieving the following objectives:

2.1.1. Strategic Security Objectives

The Company is dedicated to securing its digital assets, infrastructure, and information across all platforms and business functions. To fulfill this commitment, the Company will ensure clear communication of its strategic and operational approach to information security, encompassing all personnel, contractors, vendors, and third parties who access, process, store, or manage its data and systems.

Responsibilities and obligations will be explicitly defined for all individuals involved in managing the Company's information assets. Protecting personal, operational, financial, and customer data from unauthorized access, disclosure, loss, alteration, or misuse is a priority, with a focus on compliance with the General Data Protection Regulation (GDPR) and other relevant laws.

The Company will also maintain the accuracy and reliability of its data and systems, ensuring that betting systems, customer transactions, reporting, and decision-making processes are trustworthy and secure. In support of this, structured guidance will be provided for the implementation of security controls, procedures, and practices, with the aim of mitigating information-related risks to acceptable levels.

Legal and regulatory compliance, including adherence to the laws of Curaçao, GDPR, and industry-specific regulations such as Anti-Money Laundering (AML), Know Your Customer (KYC), and responsible gaming, will be ensured across all operations.

A culture of information security awareness and accountability will be cultivated throughout the organization, empowering individuals to contribute to the security posture of the Company. Finally, the Company is committed to continuous improvement of its Information Security Management System (ISMS) through regular monitoring, risk assessments, audits, and management reviews, ensuring that security measures evolve in response to emerging threats and challenges.

2.2. Scope of Information

This Information Security Policy applies to all forms of information processed or held by the Company, whether in digital or physical format. It encompasses, but is not limited to, the following categories of information:

- **External Customer Information:** Personal, financial, and behavioral data collected and processed in relation to player accounts and betting activities.
- **Operational Documentation:** Internal communications, operational plans, business strategies, audit reports, and meeting records.
- **Financial, Legal, and Compliance Records:** Company financial statements, tax filings, regulatory reports, and Anti-Money Laundering (AML) documentation.
- **Human Resources and Employee Records:** Employment contracts, performance evaluations, health and safety records, and payroll information.

This Policy also applies to all information managed in accordance with relevant privacy, gaming, and financial regulations, including but not limited to the General Data Protection Regulation (GDPR), Know Your Customer (KYC) and Anti-Money Laundering (AML) laws, and the requirements set forth by Curaçao eGaming.

To uphold the principles set forth in this Policy, the Company is committed to achieving the following objectives:

1. **Comprehensive Risk Assessment:** Conducting regular, systematic evaluations of the organization's information security risks, considering potential threats, vulnerabilities, and impacts, in order to identify and prioritize unacceptable risks.

2. **Implementation of Security Controls:** Designing and applying a comprehensive set of information security controls, as well as other risk mitigation strategies such as risk avoidance or transfer, to address identified risks that fall outside of the Company's defined Risk Appetite.
3. **Ongoing Management and Oversight:** Adopting a structured management process to ensure that the information security controls remain effective and adapt to the changing needs and requirements of the organization.
4. **Continuous Improvement:** Ensuring the continuous enhancement of the Information Security Policy through regular monitoring, risk assessments, and updates to maintain its relevance and effectiveness in light of emerging threats and regulatory changes.

2.3 Scope of Information Systems

This policy applies to all information processing facilities within the Company, including, but not limited to, the following:

- Data Centers, Servers, and Cloud Environments: All physical and virtual infrastructure used to store, process, and manage Company data.
- Workstations, Laptops, and Mobile Devices: Any devices used for Company business, both within the workplace and remotely, that access or store Company data.
- Software Platforms, Databases, and Network Devices: All applications, databases, and network equipment used to facilitate the Company's operations and data management.
- Internal and External Communication Systems: Communication tools, such as email, VoIP, and messaging platforms, used for internal and external business interactions.

This policy covers all these facilities and systems to ensure comprehensive security and protection of the Company's information assets.

2.4 Third-Party and Outsourced Services

This Policy also extends to all external entities, including vendors, service providers, consultants, and affiliates, that:

- Provide services such as hosting, payment processing, marketing, customer support, or identity verification;
- Have access to the Company's data or infrastructure, either directly or indirectly;
- Process personal data on behalf of the Company under data processing agreements (DPAs) or contractual obligations.

These external parties are required to adhere to the same security principles and standards as outlined in this Policy to ensure the protection of the Company's information assets.

2.5 Users Covered by this Policy

This Policy applies to the following categories of users:

- Full-time and part-time employees
- Independent contractors and consultants
- Temporary staff, interns, and agency workers
- Third-party service providers with access to information assets or processing systems

For the purposes of this Policy, all of the above individuals and entities are collectively referred to as "Users."

3. Individual Responsibilities

Information security is a critical component of the Company's overall risk management and compliance framework. This section defines the roles and responsibilities of all individuals and key stakeholders involved in safeguarding information assets and maintaining the integrity of the Company's Information Security Management System (ISMS).

All users—whether internal or external—who access or interact with the Company's information systems are expected to fully understand and adhere to the responsibilities outlined in this Policy. Compliance with these responsibilities is essential for ensuring the ongoing protection of the Company's information and systems.

3.1 All Employees, Contractors, and Partners

All colleagues, contractors, consultants, and authorized third-party users are responsible for:

- Complying with this Information Security Policy, as well as all related security, privacy, and compliance procedures.
- Protecting Company information assets—such as customer data, operational documents, and system credentials—from unauthorized access, disclosure, alteration, or destruction.

- Adhering to secure usage practices for hardware, software, and communication platforms.
- Completing mandatory information security and data protection training during onboarding, and annually thereafter.
- Promptly reporting any actual or suspected security incidents, data breaches, system misuse, or policy violations through the appropriate reporting channels (e.g., internal ticketing system or directly to the Information Security Officer).
- Remaining vigilant about phishing threats, social engineering risks, and other potential cyberattack vectors.

3.2 System Users and Data Handlers

Any individual user—whether internal or external—who accesses the Company’s systems or handles Company information, whether through internal platforms or remote access, is responsible for:

- Adhering to all relevant Company policies, regulatory requirements (e.g., GDPR, AML/KYC), and contractual obligations pertaining to information security.
- Ensuring the security of access credentials (such as usernames, passwords, and API keys), and never sharing them with unauthorized individuals.
- Using Company data exclusively for authorized business purposes and ensuring its protection and proper handling.
- Immediately reporting any incidents of unauthorized access, data loss, or breaches of this Policy through the designated reporting channels.

3.3 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is appointed in accordance with the General Data Protection Regulation (GDPR) and is responsible for ensuring the Company’s compliance with data protection laws.

Key responsibilities of the DPO include:

- Overseeing and ensuring compliance with the GDPR and relevant privacy laws across all jurisdictions in which the Company operates.

- Providing guidance to internal stakeholders on conducting Data Protection Impact Assessments (DPIAs), applying privacy-by-design principles, and ensuring the lawful processing of personal data.
- Acting as the primary liaison between the Company, supervisory authorities, and data subjects.
- Supervising the management of data subject rights, including those related to access, rectification, erasure, and data portability.

4. Compliance

The Company is committed to complying with all relevant laws, regulations, and contractual obligations, including Curacao eGaming, GDPR, and AML/KYC legislation. This Policy provides a framework to prevent violations.

- All users (employees, contractors, consultants, third parties) must comply with this Policy and related procedures.

Non-compliance may result in:

- Disciplinary action, including termination of employment or contracts.
- Regulatory reporting requirements.
- Legal consequences under data protection or gambling laws.

To ensure compliance, the Company will:

- Provide ongoing training on information security, privacy, and acceptable use.
- Ensure employees understand their responsibilities and how to report potential threats or breaches.
- Regularly update training to address emerging risks and regulatory changes.

4.1. Awareness and Training

To ensure effective compliance, the Company will:

- Provide ongoing training on information security, privacy, and acceptable use for all staff.
- Ensure employees understand their responsibilities under this Policy, including identifying and reporting potential threats, breaches, or vulnerabilities.

- Regularly review training content to address emerging risks, regulatory changes, and best practices.

4.2. Monitoring and Enforcement

Compliance will be monitored through:

- Audits and system reviews.
- Ongoing risk assessments and testing.
- Investigation of security incidents and violations.

Breaches will prompt corrective actions and inform future improvements.

5. Specific Security Objectives

To manage risk effectively, the Company has adopted several operational security objectives. Controlled access ensures that information is accessible only to authorized individuals and only for as long as necessary for operational or regulatory purposes. Delegated access rights are granted based on clearly defined roles and responsibilities, with access levels enforced through centralized identity and access management tools. In addition, the Company ensures the confidentiality and integrity of its systems and data by safeguarding against unauthorized changes or disclosures.

Service availability is a priority, and all applications, including cloud-hosted platforms, are maintained in line with Service Level Agreements (SLAs) to ensure uninterrupted access and performance. To support long-term operational stability, the Company has implemented comprehensive business continuity and disaster recovery policies, which are regularly tested to ensure resilience during disruptions. Furthermore, all security and data protection policies are clearly documented and made readily accessible to staff and relevant third parties.

The Company employs a rigorous incident management process to promptly report, log, investigate, and remediate any security breaches or weaknesses. Regular audits and reviews are conducted to assess compliance and to continuously improve the security framework. When deploying new systems, applications, or services, the Company follows a structured approach, including formal risk assessments and approval processes to ensure secure deployment.

Finally, the Company's vulnerability management procedures include regular audits and testing to identify potential weaknesses, automated patch management where feasible, and a documented process for assessing, reporting, and remediating vulnerabilities within defined timeframes.

6. Oversight and Governance

The Company's Security Governance Group (or equivalent internal authority) is responsible for overseeing the performance of security objectives. This group will review the security objectives at least annually, or in response to regulatory or risk-based changes, ensuring alignment between the Company's security posture and its broader risk management strategy. Additionally, the group will monitor and evaluate risks related to confidentiality, service delivery, and the availability of information systems to ensure ongoing security and compliance.

7. Other Policies

This Policy shall be read in conjunction with the following policies and shall be deemed to form part of the Terms and Conditions.

1. AML Policy
2. Privacy Policy
3. Responsible Gaming
4. KYC Policy and Procedure