

ApexBet

Information Security Policy

1. Purpose

This Information Security Policy sets out the principles and measures through which ApexBet Gaming N.V. (hereinafter referred to as “ApexBet”) protects the confidentiality, integrity, and availability of its information assets in the context of its gambling operations.

This Policy focuses on safeguarding player data, gambling transaction data, payment information, and gambling systems against unauthorised access, use, disclosure, alteration, or destruction.

2. Scope of Application

This Policy applies to all information systems, data assets, and business processes operated or used by ApexBet, including but not limited to:

- Player personal and account data;
 - Gambling and gaming transaction data;
 - Payment, withdrawal, and funds flow information;
 - Gambling platforms, game systems, and related technical infrastructure;
 - Employees, contractors, and third-party service providers who have access to such information.
-

3. Information Security Principles

ApexBet applies the following principles in managing information security:

1. Access to information is restricted to authorised individuals based on their roles and responsibilities;
 2. Appropriate measures are implemented to ensure data accuracy and integrity;
 3. Critical systems and data are maintained in a reasonably available state;
 4. Information security controls are proportionate to identified risks;
 5. Information security measures support regulatory compliance and player protection objectives.
-

4. Information Security Governance and Responsibility

ApexBet has designated the **Compliance Officer** as the individual responsible for information security governance and oversight, in coordination with relevant technical and operational functions.

The Compliance Officer is responsible for:

1. Overseeing the implementation and ongoing effectiveness of this Policy;
2. Coordinating information security risk assessments and control measures;

3. Reviewing material information security incidents and response actions;
 4. Reporting information security matters to ApexBet's senior management where appropriate;
 5. Ensuring alignment between information security management and applicable regulatory requirements.
-

5. Information Classification and Access Control

ApexBet classifies information based on sensitivity and business criticality.

Appropriate access controls are applied to each category of information, including measures to:

- Prevent unauthorised access, disclosure, or modification;
 - Limit access to information on a need-to-know basis;
 - Apply enhanced controls to sensitive data and critical systems.
-

6. System and Data Security Measures

ApexBet implements reasonable technical and organisational measures to protect its information systems and data.

Such measures include, but are not limited to:

- Protection against unauthorised system access;
 - Prevention of data loss, leakage, or unauthorised alteration;
 - Safeguards to ensure the stability and reliability of gambling platforms and related systems;
 - Measures to minimise operational disruption in the event of system failures or security incidents.
-

7. Third-Party and Outsourced Service Management

Where ApexBet engages third-party or outsourced service providers who process or access information, ApexBet ensures that:

1. Such providers are required to comply with applicable information security and data protection requirements;
2. Security responsibilities are clearly defined in contractual arrangements;
3. Reasonable oversight is maintained over third-party compliance.

Notwithstanding the use of third parties, ApexBet retains ultimate responsibility for information security.

8. Information Security Incident Management and Notification

ApexBet maintains procedures to identify, respond to, and manage information security incidents.

Where an information security incident may materially affect player data, gambling transactions, payment systems, or the integrity of gambling platforms, ApexBet will:

1. Take timely actions to contain and mitigate the impact of the incident;

2. Record the nature, scope, and resolution of the incident;
 3. **Fulfil applicable legal and regulatory notification obligations, including notification to the Curaçao Gaming Authority where required.**
-

9. Integration with Gambling Compliance Functions

Information security measures form an integral part of ApexBet's overall compliance framework and support the effective operation of:

- Anti-money laundering and customer due diligence (AML / KYC);
 - Payment and funds security controls;
 - Responsible gaming measures;
 - Player complaint handling and dispute resolution;
 - Fraud prevention and system integrity protections.
-

10. Employee Awareness and Training

ApexBet ensures that employees with access to information systems or data maintain an appropriate level of information security awareness.

Where appropriate, employees receive information security training relevant to their roles in order to mitigate human-related security risks.

11. Policy Review and Senior Management Oversight

This Information Security Policy is reviewed for effectiveness at least **once every twelve (12) months**.

The results of such reviews are reported by the Compliance Officer to ApexBet's senior management and are used to support policy updates, resource allocation, and continuous improvement.

12. Record Keeping

Records relating to information security risk assessments, incidents, response actions, and policy reviews are retained in accordance with applicable legal and regulatory requirements and are made available to competent authorities upon request.