

Information Security Policy for FairPari.com

1. Purpose

The purpose of this policy is to establish how FairPari.com manages and protects information assets. Its objectives are to:

- Defend sensitive customer and company data against misuse or unauthorized disclosure.
 - Limit risks from cyberattacks, breaches, and operational vulnerabilities.
 - Maintain compliance with GDPR, AML, and other applicable legal and regulatory standards.
 - Enhance trust among players, partners, and regulators by demonstrating a strong commitment to information security.
-

2. Scope

This policy applies to:

- All FairPari.com staff, contractors, and external service providers.
 - All IT systems, platforms, applications, and databases managed or operated by FairPari.com.
 - Customer records, transactions, payment data, and confidential corporate information.
-

3. Key Principles

a. Confidentiality

- Sensitive data is only accessible to staff who require it for their duties.
- Access rights are protected through strong authentication and role-based controls.

b. Integrity

- Data must remain accurate, complete, and protected against unauthorized modification or deletion.
- Regular backups ensure that lost or corrupted data can be restored quickly.

c. Availability

- Services are designed to minimize downtime and ensure reliable access for users.
- Business continuity and disaster recovery procedures are maintained to handle disruptions.

d. Compliance

- All handling of customer and business information complies with GDPR, AML directives, and local regulatory obligations.

4. Security Measures

a. Network Protection

- Firewalls, intrusion prevention/detection systems, and encryption secure the FairPari.com infrastructure.
- All customer communications and transactions are encrypted via SSL/TLS.

b. Access Management

- Role-based access is enforced so staff only receive the permissions necessary for their function.
- Access is revoked without delay when contracts or employment end.

c. Data Encryption

- Customer and business-critical information is encrypted both in storage and during transmission.
- Strong, industry-accepted encryption protocols are applied consistently.

d. Endpoint Security

- Devices used to access FairPari.com systems are protected by antivirus tools, firewalls, and endpoint security solutions.
- Patch management ensures vulnerabilities are addressed promptly.

e. Monitoring and Auditing

- All system activities, such as logins and financial operations, are continuously monitored for anomalies.
- Independent audits are carried out to confirm compliance with regulations and internal policies.

f. Vendor Oversight

- Third-party service providers must comply with FairPari.com's security standards.
 - Vendors are regularly reviewed to ensure adherence to these standards.
-

5. Employee Responsibilities

All staff and contractors are required to:

- Follow the Information Security Policy and associated procedures.
- Immediately report suspected vulnerabilities, incidents, or data breaches.
- Participate in periodic training on data protection and cybersecurity awareness.

6. Incident Response and Breach Management

a. Detection and Reporting

- Security incidents are monitored for and detected continuously.

b. Response Plan

When an incident occurs, the response team will:

- Contain the issue to limit damage.
- Investigate the cause and document the findings.
- Notify regulators and affected customers if legally mandated.
- Apply corrective measures to reduce the chance of recurrence.

c. Customer Communication

- In case of a breach impacting personal data, affected users will be notified quickly with clear details and mitigation steps.

7. Risk Management

- Regular risk reviews identify new threats and vulnerabilities.
- Security strategies are updated in response to changes in technology, business operations, and regulatory frameworks.

8. Policy Enforcement and Compliance

- Employees or contractors violating this policy may face disciplinary action, up to and including termination.
- Customer violations of security protocols may result in account suspension or closure.

9. Policy Review and Updates

- The policy is reviewed annually or when significant regulatory, technical, or business changes occur.
 - Updated versions are distributed to relevant stakeholders to ensure ongoing compliance.
-