

Information Security Policy for Najahbet.com

1. Purpose

The objectives of this policy are to:

- Protect sensitive customer and organizational information.
 - Mitigate the risks associated with data breaches, cyberattacks, and unauthorized access.
 - Ensure compliance with data protection regulations such as GDPR and other applicable laws.
 - Foster trust and confidence among our players and stakeholders.
-

2. Scope

This policy applies to:

- All employees, contractors, and third-party service providers of Najahbet.com.
 - All information systems, applications, and data owned, managed, or processed by Najahbet.com.
 - Customer data, financial transactions, and any sensitive business information.
-

3. Key Principles

a. Data Confidentiality

- Access to sensitive information is restricted to authorized personnel on a need-to-know basis.
- Multi-factor authentication (MFA) and role-based access controls are used to protect systems and data.

b. Data Integrity

- All data is protected against unauthorized alteration or destruction.
- Regular backups are performed to ensure data can be restored in the event of loss or corruption.

c. Data Availability

- Systems are designed to minimize downtime and ensure continuous availability of services.
- Disaster recovery and business continuity plans are in place to address unforeseen events.

d. Regulatory Compliance

- All data handling and security measures comply with GDPR, AML regulations, and local laws.

4. Security Measures

a. Network Security

- Firewalls, intrusion detection/prevention systems, and encryption protect the network.
- All connections to the platform, including customer transactions, are secured using SSL/TLS encryption.

b. Access Control

- Employees and contractors are assigned access levels based on their roles.
- Access is revoked immediately upon termination of employment or contract.

c. Data Encryption

- Sensitive customer data, including payment information, is encrypted both in transit and at rest.
- Strong encryption protocols are used to protect all sensitive data.

d. Endpoint Security

- All devices used to access Najahbet.com systems are secured with antivirus software, firewalls, and endpoint protection solutions.
- Regular software updates and patch management ensure vulnerabilities are addressed promptly.

e. Monitoring and Auditing

- All system activity, including logins and transactions, is monitored to detect and respond to suspicious behavior.
- Regular audits are conducted to ensure compliance with security policies and regulations.

f. Third-Party Vendor Security

- Vendors and service providers are required to adhere to Najahbet.com's security standards.
- Regular assessments are conducted to ensure third-party compliance.

5. Employee Responsibilities

All employees and contractors are expected to:

- Adhere to the Information Security Policy and associated guidelines.
 - Report any suspected security incidents or breaches immediately.
 - Complete regular training on cybersecurity and data protection practices.
-

6. Incident Response and Breach Management

a. Incident Detection and Reporting

- A dedicated team monitors for security incidents 24/7.

b. Response Plan

- Upon detection of an incident, the response team will:
 - Contain the incident to prevent further damage.
 - Investigate and identify the root cause.
 - Notify affected parties and regulatory bodies, as required by law.
 - Implement corrective measures to prevent recurrence.

c. Communication

- In the event of a data breach, customers will be informed promptly, with details of the breach, its impact, and steps taken to mitigate risks.
-

7. Risk Management

- Regular risk assessments are conducted to identify and mitigate potential threats.
 - Security controls are reviewed and updated based on evolving risks and technologies.
-

8. Policy Enforcement and Compliance

- Non-compliance with this policy by employees or contractors may result in disciplinary actions, including termination of employment or contract.
 - Violations of security measures by customers may result in account suspension or closure.
-

9. Policy Review and Updates

This policy is reviewed annually or when significant changes occur in technology, regulations, or business operations. Updates will be communicated to all stakeholders.
