

Information Security Policy for Agg.bet

1. Purpose

This policy sets out Agg.bet's approach to information security with the aim to:

- Safeguard confidential customer and company information from misuse or unauthorized disclosure.
 - Reduce exposure to risks such as hacking, data loss, or unauthorized access.
 - Ensure ongoing compliance with GDPR and other relevant data protection and gaming regulations.
 - Build trust and assurance with players, partners, and regulators by demonstrating a strong commitment to security.
-

2. Scope

This policy applies to:

- All employees, contractors, and external service providers engaged by Agg.bet.
 - All platforms, systems, applications, and databases operated or managed under Agg.bet.
 - Customer records, payment transactions, financial data, and sensitive business information processed by the company.
-

3. Key Principles

a. Confidentiality

- Only authorized personnel may access sensitive data, strictly on a need-to-know basis.
- Access is secured through multi-factor authentication and role-based permissions.

b. Integrity

- Data must remain accurate and protected from unauthorized modification or deletion.
- Regular backup procedures ensure recovery capability in case of system failure or corruption.

c. Availability

- Services are designed to maintain high uptime and reliable access for users.
- Disaster recovery and continuity plans are in place to reduce downtime in emergencies.

d. Compliance

- All information handling follows GDPR, AML obligations, and other applicable legal frameworks
-

4. Security Measures

a. Network Security

- Firewalls, IDS/IPS systems, and modern encryption protect the Agg.bet infrastructure.
- All traffic, including player transactions, is secured via SSL/TLS protocols.

b. Access Management

- Role-based access ensures employees and contractors receive only the permissions required for their function.
- Accounts are revoked without delay after employment or contractual engagement ends.

c. Data Encryption

- Sensitive customer information, including payment details, is encrypted during storage and transfer.
- Only strong, industry-standard encryption protocols are used.

d. Endpoint Protection

- All devices with access to Agg.bet systems are secured with antivirus, firewalls, and endpoint security tools.
- Software patches and updates are applied in a timely manner to close vulnerabilities.

e. Monitoring and Audits

- System activity, including logins and financial operations, is continuously monitored for unusual behavior.
- Scheduled audits verify compliance with internal policies and legal obligations.

f. Vendor Security

- Third-party suppliers must meet Agg.bet's security standards.
- Regular assessments are conducted to confirm vendor compliance.

5. Employee Responsibilities

All staff and contractors are required to:

- Follow this Information Security Policy and related procedures.
- Report any suspected security incident or weakness immediately.
- Participate in regular training on cybersecurity awareness and data protection.

6. Incident Response and Breach Management

a. Detection and Reporting

- Agg.bet maintains 24/7 monitoring to identify potential incidents in real time.

b. Response Process

In case of an incident, the response team will:

- Contain the breach to prevent escalation.
- Investigate the root cause and document findings.
- Notify affected users and regulators where legally required.
- Apply corrective measures to prevent recurrence.

c. Communication

- Customers are informed promptly if their data is impacted, including details of the incident, its effect, and steps taken to mitigate risk.

7. Risk Management

- Regular security risk assessments are conducted to detect potential vulnerabilities.
- Security measures are adjusted based on identified risks, industry best practices, and emerging technologies.

8. Policy Enforcement and Compliance

- Failure by employees or contractors to comply with this policy may lead to disciplinary action, up to and including termination.
- Security violations by customers may result in suspension or closure of their accounts.

9. Policy Review and Updates

- This policy is reviewed annually or whenever there are significant changes in technology, regulations, or Agg.bet operations.
- Updates are communicated to all stakeholders to ensure continuous compliance.

(SMES) Solutions for Management Employment Support N.V.

Managing Director

29.09.2025

