

Information Security Policy

Amadeus Technology B.V.

Date:03.02.2026

Purpose:

To protect the confidentiality, integrity, and availability of the company's digital assets, game servers, player data, and intellectual property, while ensuring compliance with legal, regulatory, and contractual obligations.

Scope:

This policy applies to all employees, contractors, third-party service providers, and partners who access company systems, games, or player data.

1. User Account and Access Management

- All company accounts, including admin, development, and game-server accounts, must have unique credentials.
- Multi-factor authentication (MFA) is mandatory for all administrative and development accounts.
- Access to game servers, databases, and development tools must follow the principle of least privilege.
- Accounts must be promptly disabled when employees leave or change roles.

2. Player Data Protection

- Player personal information (PII) such as email, payment details, and login credentials must be encrypted at rest and in transit.
- Collect only the data necessary for the service.
- Comply with privacy regulations.
- Never share player data with unauthorized third parties.

3. Game and Software Security

- All game code must go through code review and automated security scans before release.
- Regular patching and updates for game servers and backend infrastructure are mandatory.
- Prevent cheating, hacking, and account abuse through anti-cheat systems and monitoring.
- Protect intellectual property, including game assets, art, and source code, from theft or unauthorized use.

4. Payment and Financial Security

- Payment processing must comply with PCI DSS standards.
- Financial data must be stored securely and only accessed by authorized personnel.
- Regular auditing of transactions to detect fraud or anomalies.

5. Incident Response

- All security incidents (data breaches, DDoS attacks, account compromises, server intrusions) must be reported immediately.
- Maintain an incident response plan including containment, investigation, recovery, and communication.
- Post-incident review must be conducted to prevent recurrence.

6. Network and Infrastructure Security

- Game servers, cloud services, and internal networks must be secured with firewalls, IDS/IPS, and proper segmentation.
- Remote access must be encrypted using VPNs or secure tunneling.
- Continuous monitoring for unusual activity, DDoS attempts, and intrusion attempts.

7. Employee Training and Awareness

- All staff must complete annual cybersecurity and data privacy training.
- Developers and engineers receive additional training on secure coding practices and anti-cheat development.
- Regular updates about phishing, malware, and emerging threats in the gaming industry.

8. Third-Party Management

- Data processors handling player data or game services must comply with company security policies.
- Contracts must include security requirements and regular audit rights.
- Periodic review of third-party systems for compliance and vulnerabilities.

9. Compliance and Legal Obligations

- Adherence to international, national, and regional regulations regarding data protection, intellectual property, and online safety.
- Non-compliance may lead to disciplinary actions, fines, or legal consequences.

10. Policy Review

- Policy will be reviewed at least annually or when there are significant changes in technology, regulations, or company operations.

11. Player Data Storage, Retention, and Localization

- All player data, including personal information, in-game assets, and transaction history, must be stored securely on company servers located in **Curacao**.
- Data must be encrypted at rest and in transit to prevent unauthorized access or breaches.

- Player data must be retained for **at least 5 years** to comply with business, legal, and auditing requirements.
- Access to stored player data is restricted to authorized personnel only, based on role and job requirements.