

INFORMATION SECURITY POLICY OF 759GAMING.COM

Last updated: 25 June 2025

Introduction:

759gaming.com is a brand name of Caribbean Vista Media B.V. This Information Security Policy outlines the principles and procedures adopted by Caribbean Vista Media B.V. to ensure the confidentiality, integrity, and availability of information assets managed by 759gaming.com, particularly in the context of online gaming development and operations.

1. Purpose and Scope:

This policy establishes a comprehensive framework to protect 759gaming.com's digital infrastructure and customer data. It applies to all employees, contractors, third-party partners, and systems interacting with 759gaming.com platforms.

2. Information Security Objectives:

- Ensure protection of game data, source code, user information, and transaction logs.
- Prevent unauthorized access, modification, or loss of data.
- Maintain compliance with applicable gaming regulations and data protection laws.
- Support operational continuity and incident response preparedness.

3. Roles and Responsibilities:

- Information Security Officer (ISO): Oversees security implementation and risk management.
- IT Department: Maintains technical safeguards and system security.
- Developers: Secure game development environments and follow secure coding practices.
- All Staff: Follow the security procedures and report security incidents immediately.

4. Access Control:

- Role-based access is enforced across systems.
- Multi-factor authentication (MFA) is required for admin systems.
- Password policies require complexity and periodic renewal.

5. Data Security and Encryption:

- Sensitive data (e.g., user credentials, payment info) must be encrypted at rest and in transit.
- Game logic and source code are stored in secure, access-controlled repositories.
- Regular data backups are performed and stored securely.

6. Game Development Security:

- Secure coding practices are mandatory for all developers.
- Code repositories are monitored for unauthorized changes.
- Version control is strictly enforced, and peer code reviews are required.

7. Incident Management:

- All incidents must be reported immediately to the ISO.
- An incident response plan (IRP) is in place and tested periodically.
- Lessons learned are documented and applied to prevent recurrence.

8. Third-Party Risk Management:

- All vendors with access to 759gaming.com systems must sign data processing agreements.
- Security audits may be conducted on third parties handling sensitive data or assets.

9. Training and Awareness:

- Security training is provided to all new employees.
- Annual refresher training is mandatory for all staff.
- Developers receive specialized training on secure development lifecycle (SDLC).

10. Compliance and Review:

This policy will be reviewed annually by Caribbean Vista Media B.V. or in the event of significant operational, legal, or technical changes. Non-compliance with this policy may result in disciplinary or legal action.