

Information Security Policy

NovaGaming B.V.

Zuikertuintjeweg Z/N, Curaçao

Effective Date: June 03, 2025

1. Objective

NovaGaming B.V., a private limited liability company incorporated under the laws of Curaçao with registration number 1643222, is dedicated to ensuring the confidentiality, integrity, and availability of its information assets. This Information Security Policy establishes a framework to protect sensitive data, intellectual property, and client information, ensuring compliance with applicable laws and industry standards in the business-to-business (B2B) gaming sector.

2. Scope

This policy applies to:

- All information systems, networks, applications, and devices owned, managed, or utilized by NovaGaming B.V.
- All data processed by the company, including but not limited to client data, game development materials, financial records, and intellectual property.
- All personnel, including employees, contractors, consultants, third-party vendors, and partners, who access or interact with NovaGaming B.V.'s information assets.

3. Governance

3.1 Roles and Responsibilities

- **Information Security Officer (ISO):** Responsible for overseeing the implementation, enforcement, and periodic review of this policy.
- **Senior Management:** Ensures sufficient resources and support for information security initiatives.
- **Employees and Contractors:** Must adhere to this policy and report any security incidents or policy violations promptly.

4. Security Controls

4.1 Access Management

- Access to information systems and data shall be granted based on the principle of least privilege, ensuring personnel only access resources necessary for their roles.

- Multi-factor authentication (MFA) is mandatory for all critical systems and remote access.
- Access rights shall be reviewed quarterly, with inactive accounts disabled within 30 days of inactivity.

4.2 Data Protection and Privacy

- Sensitive data, including client information, game assets, and financial records, shall be encrypted at rest and in transit using industry-standard protocols (e.g., AES-256 for encryption at rest, TLS 1.3 for data in transit).
- Data retention shall comply with legal and regulatory requirements, with secure disposal of data no longer required.
- Critical data shall be backed up regularly, with backups encrypted and stored in a secure, geographically separate location.

4.3 Incident Management and Response

- A documented Incident Response Plan shall be maintained and tested annually to ensure effective handling of security incidents, including data breaches and system compromises.
- All security incidents must be reported to the Information Security Officer within 24 hours of detection.
- A root cause analysis shall be conducted post-incident, with corrective actions implemented to prevent recurrence.

4.4 Personnel Security

- All personnel shall undergo mandatory information security training upon onboarding and annually thereafter, covering topics such as phishing, social engineering, and secure data handling.
- Use of personal devices for company business is strictly prohibited unless explicitly authorized and secured with company-approved endpoint protection solutions.
- Personnel are required to report any suspicious activity or policy violations immediately.

4.5 Third-Party Risk Management

- Third-party vendors and partners shall be required to execute a Non-Disclosure Agreement (NDA) and comply with NovaGaming B.V.'s information security requirements.
- Third-party access to systems shall be monitored, logged, and revoked immediately upon termination of engagement.
- Annual assessments of third-party compliance with security standards shall be conducted.

4.6 Compliance and Auditing

- NovaGaming B.V. shall comply with all applicable legal and regulatory requirements, including but not limited to data protection laws in Curaçao and the European Union (e.g., GDPR, where applicable).
- Internal audits of information security practices shall be conducted annually, with findings and remediation plans reported to senior management.
- External audits may be performed as required to validate adherence to industry standards and contractual obligations.

5. Policy Compliance

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual agreements, and potential legal action in cases of gross negligence or willful misconduct.
- Compliance with this policy is mandatory for all personnel and third parties interacting with NovaGaming B.V.'s information assets.

6. Policy Review and Amendments

- This policy shall be reviewed annually or upon significant changes in the regulatory, technological, or business environment.
- Amendments to the policy shall be approved by senior management and communicated to all relevant stakeholders.

7. Point of Contact

For inquiries, incident reporting, or clarification regarding this policy, please contact:

Director

NovaGaming B.V.

Zuikertuintjeweg Z/N, Curaçao

Email: admin@novagaming888.com

Last Reviewed: June 03, 2025

Version: 1.0