

Information Security Policy B2C

Novisoft N.V.

Document Control

Version	Date	Description of Changes	Author
1.0	21.05.2026	Initial draft	IGA Trust B.V.

--	--	--	--

1. Purpose

This Information Security Policy establishes the minimum security requirements for the protection of systems, player information, gaming platforms, financial data, and operational processes used by the Company as a B2C gaming operator.

The policy is designed to:

- Protect confidentiality, integrity, and availability of information assets
- Support compliance with applicable gaming regulations and licensing obligations
- Reduce cybersecurity risks affecting players, partners, and operations
- Support alignment with ISO/IEC 27001:2022 and CIS Controls

2. Scope

This policy applies to:

- All employees, contractors, consultants, and third parties
- All information systems, gaming platforms, applications, infrastructure, and cloud services
- All player data, payment data, gaming transaction data, and operational records
- All physical and remote working environments

3. Roles and Responsibilities

3.1 Executive Management

Executive management shall:

- Approve and support the information security program

- Ensure sufficient resources are available
- Review security risks and compliance status regularly

3.2 Information Security Officer

The Information Security Officer shall:

- Maintain security policies and procedures
- Coordinate security monitoring and incident response
- Oversee vulnerability management and compliance activities

3.3 Employees and Contractors

Personnel shall:

- Follow security policies and procedures
- Report incidents or suspicious activity immediately
- Protect credentials and sensitive information

4. Asset Management

The Company shall:

- Maintain an inventory of all hardware, software, cloud assets, and gaming systems
- Classify information assets according to sensitivity
- Assign ownership for critical systems and data
- Review asset inventories periodically

5. Access Control

The Company shall:

- Implement role-based access controls (RBAC)
- Apply least privilege principles
- Require management approval for access requests
- Remove or modify access immediately upon role change or termination
- Enforce multi-factor authentication for:

- Administrative access
- Remote access
- Internet-facing systems

Password Requirements:

- Minimum 14 characters for accounts without MFA
- Minimum 8 characters for accounts protected by MFA
- Shared accounts are prohibited unless formally approved and monitored

6. Data Protection

The Company shall:

- Encrypt sensitive data at rest and in transit
- Apply secure retention and disposal procedures
- Use data masking in non-production environments
- Protect player credentials, financial data, and gaming records

Retention:

- Gaming transaction records shall be retained according to applicable regulatory requirements
- Secure disposal methods shall include deletion, cryptographic erasure, or physical destruction

7. System Security

The Company shall:

- Apply secure configuration standards to all systems
- Disable unnecessary services and default accounts
- Use secure management protocols such as SSH and HTTPS
- Deploy centrally managed anti-malware protection
- Implement firewalls and endpoint protection controls

8. Vulnerability and Patch Management

The Company shall:

- Perform regular vulnerability scanning
- Prioritize remediation based on risk
- Apply security patches monthly or earlier for critical vulnerabilities
- Test updates before deployment into production

9. Logging and Monitoring

The Company shall:

- Enable audit logging on critical systems
- Retain logs according to regulatory and operational requirements
- Protect logs from unauthorized access or modification
- Monitor logs for suspicious activity

Gaming-specific logs shall include:

- Player activity
- Betting and transaction records
- Administrative changes
- Financial movements

10. Third-Party Management

The Company shall:

- Maintain a register of all third-party providers
- Assess security risks before onboarding vendors
- Include security obligations in contracts
- Monitor the certification and compliance status of B2B providers

Additional controls for gaming suppliers and data feeds:

- Encrypted and authenticated communications

- Integrity validation of data feeds
- Incident notification obligations
- Defined failover procedures

11. Incident Response

The Company shall:

- Maintain an incident response plan
- Assign incident response roles and escalation paths
- Maintain an up-to-date incident contact list
- Report regulatory incidents within required timeframes

Reportable incidents include:

- Compromise of player data
- Gaming integrity incidents
- System outages affecting regulated operations
- Security breaches impacting financial systems

12. Backup and Recovery

The Company shall:

- Perform automated backups of critical systems and data
- Protect backup data using encryption and access controls
- Test restoration procedures periodically
- Define recovery time objectives (RTOs) and recovery point objectives (RPOs)

13. Security Awareness and Training

The Company shall:

- Deliver security awareness training during onboarding
- Conduct annual refresher training
- Provide role-specific training for high-risk functions

- Conduct phishing and social engineering simulations

14. Physical Security

The Company shall:

- Restrict access to secure areas
- Use CCTV and access logging where appropriate
- Protect gaming equipment and infrastructure
- Secure company assets used off-site

15. Compliance and Governance

The Company shall:

- Maintain compliance with applicable gaming laws and regulations
- Conduct periodic reviews of security controls
- Review this policy annually or following significant changes
- Maintain documentation supporting audits and inspections

16. Enforcement

Violations of this policy may result in:

- Disciplinary action
- Suspension of access privileges
- Contract termination
- Legal or regulatory reporting where applicable