

Niollo B.V.

Information Security Policy

Date: 5 May 2026

Version 1.0

Table of Contents

1. Purpose and Scope	2
2. Governance and Responsibilities	2
3. Risk Management Framework.....	2
4. Data Governance and Protection	3
4.1 Data Classification and Handling	3
4.2 Data Protection and Privacy.....	3
4.3 Data Retention and Deletion.....	3
4.4 Audit Logging	3
4.5 Backups.....	3
5. Access Control	4
6. System and Network Security	4
7. Software Development and Change Management	4
8. Incident Management and Response	5
9. Business Continuity and Disaster Recovery	5
10. Third-Party and Vendor Security	5
11. Staff Responsibilities and Awareness	6
12. Monitoring, Audit and Continuous Improvement	6
13. Exceptions.....	6
14. Non-Compliance	6

1. Purpose and Scope

The Information Security Policy (this “Policy”) establishes the governance framework for the protection of information assets for Niollo B.V. (the “Company”) and its affiliated entities. It defines the principles, controls, and responsibilities required to safeguard information systems, data, and operational infrastructure against security threats, ensuring confidentiality, integrity, availability, and regulatory compliance.

The Policy applies to all employees, contractors, third-party providers, systems, and data processed, stored, or transmitted within the Company’s environment. This includes cloud services, on-premise systems, remote working environments, and outsourced infrastructure.

The Policy is designed to reflect the Company’s operational model, including its reliance on third-party providers, gaming platforms, and distributed infrastructure.

2. Governance and Responsibilities

Overall accountability for information security rests with the CyberSecurity Specialist, who endorses and approves this Policy.

Operational responsibility is structured as follows:

- The CyberSecurity function is responsible for designing, implementing, and maintaining the information security framework. It oversees risk management, incident response, and technical security controls.
- Corporate IT is responsible for day-to-day system administration, access provisioning, infrastructure security, and monitoring activities.
- Management is responsible for ensuring that security requirements are implemented within their respective business areas and that staff comply with this Policy.

All employees and contractors are responsible for adhering to security requirements, reporting incidents, and handling data in accordance with its classification.

Policy updates are reviewed at least annually or following material changes in systems, risks, or regulatory expectations.

3. Risk Management Framework

The Company maintains a structured risk management process to identify, assess, and mitigate information security risks.

Risk assessments are conducted at least annually and upon significant system or operational changes. These assessments consider threats such as cyberattacks, insider misuse, fraud, phishing, ransomware, data leakage, system failures, and third-party risks.

Risks are documented in a risk register, which includes impact assessments, mitigation actions, responsible owners, and review timelines. Remediation actions are tracked to completion and subject to management oversight.

The risk management process ensures alignment between the value of information assets and the level of protection applied.

4. Data Governance and Protection

4.1 Data Classification and Handling

All data is classified according to sensitivity and business impact using a structured classification model ranging from public to highly restricted data. Data handling requirements are aligned to classification levels and include access restrictions, storage controls, transmission safeguards, and retention rules.

4.2 Data Protection and Privacy

The Company processes personal and sensitive data in accordance with applicable data protection laws and internal privacy requirements. Personal data includes customer, employee, financial, and operational data, as defined in the Company's privacy framework.

Encryption is applied where appropriate for data at rest and in transit. Access to sensitive data is limited based on role and business need.

4.3 Data Retention and Deletion

Data is retained only for as long as necessary for business or legal purposes and is securely deleted or anonymised when no longer required.

4.4 Audit Logging

All critical systems generate audit logs capturing user activity, system changes, and access events. Logs are protected from tampering and reviewed periodically.

4.5 Backups

Data backups are performed daily or in line with system criticality. Backup integrity and restoration capabilities are tested regularly, with documented evidence of test results .

5. Access Control

Access to systems and data is managed through a formal identity and access management framework, where access is granted based on role-based principles and least privilege. All access requests require formal approval and are recorded.

User lifecycle management includes onboarding, role changes, and termination processes, ensuring timely provisioning and de-provisioning of access rights.

Privileged access is subject to additional controls, including enhanced approval and monitoring.

Periodic access reviews are conducted to ensure that access rights remain appropriate. Evidence includes access logs, approval records, and review documentation.

Multi-factor authentication is implemented for critical systems where feasible.

6. System and Network Security

The Company maintains layered technical controls to protect its infrastructure.

Network security includes firewalls, network segmentation, secure configurations, and monitoring tools.

Endpoint protection measures include anti-malware, device hardening, and patch management.

Vulnerability management is performed regularly, including scanning, remediation, and tracking of identified weaknesses.

Cloud environments are secured through configuration standards, access controls, and monitoring mechanisms.

Secure protocols and encryption are used for communications and data transfer.

7. Software Development and Change Management

Changes to systems are governed by a formal change management process, where all changes are documented, risk-assessed, tested, and approved prior to deployment. Where applicable, rollback procedures are defined.

Security considerations are integrated into the development lifecycle, including code reviews and testing.

8. Incident Management and Response

The Company maintains an incident response framework for identifying, managing, and reporting security incidents. Incidents include data breaches, cyberattacks, system outages, fraud events, and any threats to system integrity.

Incidents are reported immediately to the CyberSecurity function, escalated based on severity, and managed through defined response procedures.

Post-incident reviews are conducted to identify root causes and implement corrective actions.

Incident records are maintained, including timelines, actions taken, and lessons learned.

Where required, incidents are notified to the Compliance Team and subsequently reported to the Corporate Director of the Company, as well as the Curacao Gaming Authority in accordance with applicable obligations. Such reporting also includes security breaches and system failures.

9. Business Continuity and Disaster Recovery

The Company maintains a Business Continuity and Disaster Recovery framework to ensure operational resilience. Critical systems are identified through business impact analysis, with defined recovery objectives and restoration procedures.

Backups are stored securely and tested regularly and disaster recovery environments are maintained to support failover in case of major incidents.

Recovery processes are tested periodically to ensure effectiveness, with documented evidence of results.

Escalation procedures ensure timely communication to management and regulators in the event of major disruptions.

10. Third-Party and Vendor Security

Third-party service providers are subject to due diligence and ongoing monitoring to ensure they meet the Company's security requirements.

Contracts include security obligations, data protection provisions, and incident notification requirements.

Outsourced services are assessed for risk, and appropriate controls are implemented to mitigate third-party exposure.

11. Staff Responsibilities and Awareness

All staff must comply with acceptable use, data handling, and security requirements when accessing Company systems and data.

Security awareness training is provided regularly to ensure staff understand risks, responsibilities, and reporting obligations. Staff must immediately report any suspected or actual security incident.

Disciplinary measures apply in cases of non-compliance with this Policy.

12. Monitoring, Audit and Continuous Improvement

The Company monitors compliance with this Policy through internal reviews, audits, and system monitoring. Audit activities include review of access controls, logs, incident records, and risk management processes.

Findings are documented and tracked to resolution.

The Policy and associated controls are reviewed at least annually and updated as necessary to reflect evolving risks, technologies, and regulatory expectations.

13. Exceptions

Any exception to this Policy must be formally requested, risk-assessed, approved by the relevant authority, and documented. Exceptions are subject to periodic review.

14. Non-Compliance

Failure to comply with this Policy may result in disciplinary action, contractual penalties, or regulatory consequences, depending on severity.