Information Security Policy

Numidia B.V.

Signature CEO on behalf of BOD:
Version: 2026 – V1
Date: 07-10-2026

Index

1. Introduction 3
2. Scope and applicability 5
3. Risk based approach to information security 6
4. Information security objectives and planning 7
5. Continual improvement of the isms 9
6. Compliance and enforcement 10
7. Approval and review 11

1. Introduction

This document defines the Information Security Policy and describes how the Information Security Management System (ISMS) is established, implemented, maintained, monitored, reviewed, and continually improved within Numidia.

Information security is a critical enabler for Numidia's business operations. The organization relies extensively on information, information systems, and digital technologies to support the sourcing, trading, storage, transport, quality assurance, customer service, and support activities related to dairy ingredients and associated business processes. These information assets include, but are not limited to, customer data, intellectual property, production data, employee information, supplier information, and operational systems.

Protecting information assets is essential to:

- Safeguard business continuity and operational resilience
- Maintain customer trust and contractual compliance
- Protect intellectual property and competitive advantage
- Ensure compliance with applicable legal and regulatory requirements
- Support sustainable growth and long-term business objectives

While no management system can guarantee absolute security, the ISMS provides a structured, risk-based framework for managing information security in a consistent and measurable manner. Through this framework, Numidia aims to proactively reduce risks, improve security maturity, and respond effectively to information security incidents when they occur.

Numidia has decided to establish, implement, maintain, and continually improve an Information Security Management System (ISMS) aligned with ISO/IEC 27001 requierements. Through its ISMS, Numidia is committed to protecting the confidentiality, integrity, and availability of information and to satisfying all applicable legal, regulatory, contractual, and other information security requirements. This demonstrates that information security is managed in accordance with internationally recognized best practices and provides assurance to customers, partners, and other interested parties.

2. Scope and applicability

The Information Security Management System of Numidia B.V. covers all activities related to the sourcing, trading, quality assurance, logistics coordination, sustainability, compliance, and support functions associated with dairy ingredient trading, including all personnel, locations, information assets, supporting technologies, and business processes used to deliver these services.

This policy applies to the full ISMS scope and to all persons acting on behalf of Numidia B.V., including directors and management, employees, temporary workers, contractors, consultants, interns, suppliers, and other third parties with authorized access to Numidia information or systems.

The scope includes electronic, physical, and verbal information; all offices and operational locations belonging to Numidia B.V.; approved remote-working arrangements; on-premises systems; cloud services; outsourced IT services; end-user devices; networks; business applications; databases; and third-party hosted environments used to support business operations.

No business functions, departments, operational locations, or supporting information systems that materially contribute to the delivery of Numidia B.V.'s services are excluded from the ISMS scope. Any future exclusion shall be formally documented, justified, approved by management, and reviewed through the ISMS governance process.

All persons and relevant third parties within this applicability are required to comply with this policy and the supporting information security policies and procedures.

3. Risk based approach to information security

Numidia applies a consistent and documented **risk-based approach** to information security management. The purpose of this approach is to ensure that information security risks are identified, evaluated, and treated in a manner proportionate to their potential impact on the organization.

Information security risks are assessed in relation to the confidentiality, integrity, and availability of information assets. Risk management activities are integrated into:

- Strategic and operational planning
- Design, acquisition, and implementation of new or changed systems and services
- Change management and configuration management processes
- Supplier and third-party management
- Business continuity and resilience planning

Risk assessments are performed at planned intervals and upon significant organizational, technological, or environmental change. Risk treatment decisions are documented and result in the implementation of appropriate organizational, technical, physical, and procedural controls.

Residual risks are reviewed and accepted by appropriate levels of management. The effectiveness of risk treatment measures is monitored and reviewed as part of ongoing ISMS operation and management review activities.

4. Information security objectives and planning

Numidia establishes information security objectives to ensure that information security supports business goals, risk management priorities, and compliance obligations.

High-level information security objectives include:

1. **Protection of information assets**
   Ensure that information assets are appropriately protected against unauthorized access, disclosure, alteration, or loss, in line with their classification and business value.
2. **Operational continuity and resilience**
   Minimize the impact of information security incidents on business operations by ensuring adequate availability, backup, recovery, and incident response capabilities.
3. **Risk management effectiveness**
   Identify, assess, and treat information security risks in a structured and consistent manner, ensuring that risks remain within acceptable levels.
4. **Legal, regulatory, and contractual compliance**
   Ensure ongoing compliance with applicable laws, regulations, and contractual information security requirements, including data protection and cybersecurity obligations.
5. **Supplier and third-party security**
   Manage information security risks arising from suppliers and third parties by applying appropriate due diligence, contractual controls, and ongoing monitoring.
6. **Security awareness and competence**
   Increase awareness and competence in information security among employees and relevant third parties to reduce the likelihood of human error and policy violations.
7. **Secure use of technology**
   Ensure that information systems, including cloud and outsourced services, are designed, configured, and operated securely throughout their lifecycle.
8. **Continuous improvement of security maturity**
   Continuously improve the effectiveness and maturity of the ISMS based on audits, incidents, metrics, and feedback from interested parties.

Planning and monitoring of objectives:

- Established within a defined planning framework aligned with business and budget cycles
- Documented with responsibilities and evaluation methods
- Monitored through management reviews, audits, and performance indicators
- Updated as necessary to reflect changes in risks, technology, or business strategy

5. Continual improvement of the isms

Numidia is committed to the continual improvement of the ISMS to ensure that it remains effective, relevant, and proportionate to the organization's risk profile.

Continual improvement activities include:

- Identifying and addressing nonconformities and incidents
- Analyzing root causes and implementing corrective actions
- Improving controls, processes, and documentation
- Reviewing and enhancing performance indicators and metrics
- Incorporating lessons learned and feedback from interested parties

Improvement opportunities may be identified through audits, risk assessments, incident reviews, performance monitoring, employee feedback, customer input, or changes in business or technology. Improvement actions are prioritized, tracked, and reviewed for effectiveness.

6. Compliance and enforcement

Compliance with this policy and all supporting information security documents, standards, and procedures is mandatory for all personnel and relevant third parties.

Failure to comply may result in disciplinary measures, contractual consequences, or other actions in accordance with applicable policies and agreements. Non-compliance, incidents, or suspected weaknesses must be reported promptly to enable timely investigation and corrective action.

Management supports a culture in which compliance, transparency, and responsible reporting of information security concerns are encouraged and reinforced.

7. Approval and review

This information security policy is approved by the BOD. It is reviewed at planned intervals and whenever significant changes occur to ensure that it remains suitable, adequate and effective.

This Information Security Policy shall be communicated to all employees and relevant third parties acting on behalf of Numidia. The policy shall be made available to relevant interested parties upon request and shall be maintained as documented information within the Information Security Management System.