Nucleaire Energie Organisatie Nederland

DOCUMENT SUMMARY	
Project	Company Development
Department	GEN – General Administration
Workstream	IM/IT
Document Title	Information security policy
Document Number	2026.NNB.EF03.010.V0.2
Document Type	Policy
Revision	R0
Classification	Public

APPROVAL FORM		
Prepared by	Signature	
	Name	
	Date	February 2026
Reviewed by	Signature	
	Name	EA
	Date	February 2026
Approved by	Signature	
	Name	NEO NL management team
	Date	

REVISION HISTORY

Rev	Issue Date	Description of Changes	Author	Reviewer	Approver
0.1	February 2026	*Made concept*	*CISO*		
0.9	*February 2026*	*Reviewed concept*	*Reviewed concept*	*EA*	

Information security policy

Policy document
Level of confidentiality: Public

20 February 2026

Content

Revision and evaluation

This policy is reviewed periodically and when significant changes occur in:

- Legal or regulatory requirements
- Organisational structure

- Technology environment
- Threat landscape
- A major or significant incident

This policy is approved by the NEO NL management team and applies organization wide.

Reviewers: please make text suggestions instead of comments.

1 Introduction

1.1.1 Scope

Information security applies to both digital and physical information. This policy applies to:

- All information created, processed, stored, or transmitted by NEO NL
- All employees, contractors, suppliers, and partners
- All digital and physical information assets
- All IT, OT, cloud, and integration environments
- The full lifecycle of the programme and future operations

1.1.2 Objectives

This policy establishes the principles, direction, and governance for protecting information within NEO NL. It defines management intent and forms the foundation of the Information Security Management System (ISMS), aligned with ISO/IEC 27001, NIS2, the Dutch Cyberbeveiligingswet (Cbw), nuclear security obligations, and applicable regulatory requirements.

1.1.3 The ISMS ensures that:

- Confidentiality, integrity, and availability of information are protected
- Unauthorized access, manipulation, loss, or disclosure is prevented
- Critical operations can continue during and after disruptions
- Legal, regulatory, and contractual obligations are met
- Information remains trustworthy and usable throughout the lifecycle
- Strategic digital autonomy and operational control over critical systems are preserved

Information is treated as a strategic and safety-relevant asset and protected accordingly.

1.1.4 Strategic Alignment

This policy supports NEO NL's strategic objective to maintain operational, technical, and digital sovereignty for safety-critical and regulated functions. This ensures resilience against supply chain disruption, geopolitical instability, and systemic third-party dependency risks.

The policy further supports the strategic objective to maintain operational, technical, and digital sovereignty for safety-critical and regulated functions. This ensures resilience against:

- Supply chain disruption
- Geopolitical instability
- Concentration risk in external service providers
- Systemic third-party dependency

1.1.5 The policy reflects the following core principles:

- Safety and compliance first
- Cybersecurity and resilience are non-negotiable
- Security by design and by default
- Information as a strategic asset
- Transparency, traceability, and auditability
- Digital sovereignty and controlled dependency

1.1.6 Risk-based approach

NEO NL applies a structured risk management approach:

- Risks are identified, assessed, and treated systematically
- Risk ownership resides in the business
- The organization maintains a low-risk appetite for safety, compliance, cybersecurity, and sovereignty risks
- NEO NL maintains an up-to-date inventory of information assets, systems, and critical dependencies, including designated owners and classification levels (CMDB).
- Security and control measures are proportionate to risk and asset criticality
- Dependency risks, including supplier concentration and identity trust anchoring risks, are explicitly assessed.

1.1.7 Business Continuity and Crisis Preparedness

NEO NL maintains and periodically tests business continuity and disaster recovery capabilities to ensure continued operation of critical processes. Continuity capabilities must be demonstrably effective and not merely documented. Executive management shall review the results of annual continuity testing and confirm adequacy of resilience capability. At minimum:

- Business Continuity Plans (BCP) and IT Disaster Recovery Plans (DRP) shall be tested at least annually.
- Tests shall include realistic disruption scenarios proportionate to the Design Basis Threat (DBT) and dependency risks.
- Test outcomes shall be documented, evaluated, and reported to management.
- Identified deficiencies, improvement actions, and structural weaknesses shall be formally assigned, tracked, and implemented within defined timelines.

1.1.8 Related documents

- Classification policy (link)
- New systems policy (link)

2 Chapters the Security Policy

2.1 Governance and responsibilities

Information security governance follows the Three Lines model.

- Executive management: Accountable for information security and ISMS effectiveness
- CIO: Responsible for secure operation of IT services and control implementation
- CISO: Responsible for security strategy, policy framework, oversight, and reporting
- Information Owners: Responsible for classification, lawful processing, protection requirements, and impact assessment.
- Application/System Owners: Responsible for security, lifecycle management, dependency risk evaluation, and compliance with sovereignty requirements.

2.2 Core security principles

The following principles apply across the organization:

- Security by design and by default: New systems and processes must be compliant and secure before production use.
- Least privilege and identity-based access: Access is granted based on role, need, and accountability.
- Identity governance is centralized, lifecycle-controlled, and linked to HR processes.
- Lifecycle protection: Information and systems must remain protected throughout design, construction, operation, and decommissioning.
- Supply chain security: Security requirements apply to suppliers, contractors, and partners.
- Auditability and traceability: Security-relevant actions must be logged and be verifiable.
- Resilience: We are aware that we cannot with any degree of certainty prevent breaches. Therefor our ability to detect, respond to, and recover and learn from incidents is paramount.

2.3 Digital Sovereignty and Strategic Control

NEO NL recognizes digital sovereignty as a foundational security and resilience principle. Digital sovereignty means that the organization retains effective technical, operational, and governance control over its most critical systems, identities, cryptographic keys, and security-relevant data.

In support of this principle:

2.3.1 Layered Sovereignty Architecture

Information systems are categorized according to criticality and dependency impact. Systems supporting safety, nuclear security, regulatory obligations, cryptographic trust anchors, engineering data, or other mission-critical processes are subject to enhanced sovereignty and control requirements.

Higher-criticality systems shall:

- Be deployable on infrastructure under organizational control
- Avoid single-vendor lock-in where this creates systemic risk

- Maintain documented exit-plan and migration strategies
  - Be technically portable within defined recovery time objectives

2.3.2 Primary Identity Ownership

NEO NL maintains organizational control over primary digital identities of all personnel.

- A centrally governed primary IAM domain acts as the authoritative source of identity, linked to HR lifecycle processes.
- Access to high-criticality systems requires authentication via this primary identity domain with strong, organization-controlled multi-factor authentication.
- External or platform IAM services (e.g., commodity cloud identity services) may be used, but only as federated or derived identities, not as the primary trust anchor for critical systems.

2.3.3 Cryptographic Sovereignty

Cryptographic keys supporting critical processes, secure work environments, or regulated environments shall remain under organizational governance and technical control.

Where applicable:

- Key material shall be managed in organization-controlled trust domains.
- Reliance on exclusive third-party key management services for safety- or security-critical trust chains shall be avoided unless risk-assessed and explicitly approved.

2.3.4 Workload Portability and Continuity

Critical systems shall be architected to allow controlled relocation or recovery to alternative infrastructure environments in case of supplier disruption, geopolitical risk, or prolonged service outage.

Technical design principles supporting this include:

- Logical isolation between commodity IT and sovereign-controlled environments
- Use of standardized, portable deployment mechanisms
- Controlled federation between identity domains
- Defined emergency transition procedures

2.3.5 Controlled Federation

Where multiple security levels or environments exist, identity federation shall flow from the organization-controlled primary IAM toward lower-criticality or commodity platforms. Reverse trust dependency from critical environments to external IAM providers is not permitted without formal risk acceptance.

2.4 Insider risk and Design Basis Threat (DBT)

NEO NL recognizes that security risks may originate not only from external threat actors but also from insiders, including employees, contractors, and trusted partners with legitimate access. Insider risk, whether intentional or unintentional, is addressed through background screening where applicable, clear accountability, segregation of duties, monitoring, and the principle of least privilege. In addition, security measures are aligned with the Design Basis Threat (DBT) applicable to nuclear facilities, ensuring that protective controls, detection capabilities, and response arrangements are proportionate to credible

threat scenarios, including state-level adversaries and trusted-access misuse. This risk perspective is embedded in system design, access management, and operational oversight.

2.5 All information shall be:

- Classified at creation or first use
- Protected according to its classification
- Accessed on a need-to-know basis
- Managed throughout its lifecycle

The detailed handling requirements are defined in the Data Classification & Information Protection Policy. (link)

2.6 Information classification

All information shall be classified by its Information Owner according to sensitivity, impact, and regulatory relevance.

NEO NL applies the following classification levels:

- Public
  Information approved for public release. Disclosure causes no harm.
- Internal
  Routine business information intended for internal use. Unauthorized disclosure may cause limited operational or reputational impact.
- Restricted
  Sensitive information where unauthorized disclosure could negatively affect operations, project execution, or security posture.
- Confidential
  Highly sensitive information where unauthorized disclosure could cause significant harm to safety, security, commercial position, or regulatory compliance.
- Secret
  Information formally classified under national security regulations and subject to statutory protection requirements.

2.7 Security assurance for new and changed systems

All new information systems, applications, infrastructure components, and major system changes must comply with NEO NL security and continuity requirements before being put into production. Systems that do not meet security or sovereignty requirements require documented risk acceptance by accountable management.

Security, resilience, compliance, and continuity shall be assessed through a formal onboarding process including:

- System ownership assignment
- Risk assessment
- Business impact analysis

- Business Continuity Plans and Disaster Recovery Plans are updated. If it concerns critical systems BCP and DR are tested
- Security testing (Penetration test)
- Formal approval prior to go-live
- Approved by architecture

Detailed requirements and go/no-go criteria are defined in the policy “Security and Continuity Assurance for New Systems.” (link)

2.8 Compliance

Compliance is embedded by design in systems and processes. NEO NL maintains formal incident reporting procedures in line with NIS2 and national regulatory requirements. Significant incidents shall be reported to competent authorities within legally prescribed timeframes. Internal escalation procedures ensure timely management visibility and decision-making. NEO NL complies with applicable:

- Laws and regulations
- Nuclear safety and security obligations and Design Basis Threat (DBT) alignment
- NIS2 requirements for essential infrastructure and risk management, supply chain security, and operational resilience.
- Cyberbeveiligingswet (Cbw) the Dutch implementation of the NIS2
- Critical Entities Resilience Directive implemented by the Wet weerbaarheid kritieke entiteiten (Wwke).
- Contractual and supply chain requirements
- International standards including ISO/IEC 27001 and related frameworks

2.9 Awareness and competence

Security awareness forms part of the safety culture. All personnel must:

- Understand their responsibilities for protecting information
- Follow security policies and procedures
- Participate in awareness and training activities

2.10 Continuous improvement

The organization aims to operate at a process maturity level where risks are known, processes are defined, and controls are demonstrably effective. This corresponds to Capability Maturity Model level 3 (“Defined”), meaning that security processes are standardized, documented, consistently implemented across the organization, and their effectiveness can be validated and monitored. The ISMS is continuously improved through:

- Risk assessments
- Monitoring and measurement
- Audits and reviews
- Incident learning
- Maturity development

3 Implementation and monitoring

This chapter describes how the Information Security Policy is implemented within NEO NL, and how adherence to this policy is monitored.

3.1.1 Implementation

This policy is implemented as part of the establishment and operation of the NEO NL Information Security Management System (ISMS). Implementation takes place through the development, approval, and rollout of supporting standards, procedures, and control measures that translate this policy into daily practice. Implementation is phased and aligned with the growth of the organization, the development of the digital environment, and the onboarding of systems and suppliers.

3.1.2 Key implementation activities include:

- Formal approval and communication of the policy by executive management
- Integration of policy requirements into project governance, system development, procurement, and operational processes
- Appointment of Information Owners, System Owners, and other security responsibilities
- Embedding security-by-design in new systems, processes, and supplier engagements
- Implementation of risk management, access control, classification, and incident response practices
- Awareness and training activities to ensure that employees and contractors understand their responsibilities

Executive management is responsible for ensuring that the policy is adopted organization wide.

- The CIO is responsible for implementation within IT operations and service delivery.
- The CISO is responsible for translating this policy into the security framework, guidance, and supporting controls.
- Line management is responsible for implementation within their domains and teams.

3.1.3 Monitoring

Adherence to this policy is monitored as part of normal ISMS governance, risk management, and internal control activities. Line management is responsible for monitoring compliance within their own domains and for periodic compliance reporting. Each domain reports on the implementation and adherence to this policy through structured monthly- or periodic reports, including relevant risks, incidents, deviations, and improvement actions. Executive management is responsible for ensuring that compliance reporting takes place and that identified issues are addressed.

- Executive management shall periodically review ISMS performance, risk posture, incident trends, and resilience capability to ensure continued suitability, adequacy, and effectiveness.
- The CISO receives these periodic compliance reports, reviews and assesses them in the context of the overall security posture, and uses them to provide independent oversight, risk insight, and advice to senior management.
- Internal audit provides independent assurance on the effectiveness of controls, governance, and adherence to the policy.

Monitoring activities include:

- Periodic risk assessments and control evaluations
- Internal audits and management reviews
- Security maturity monitoring and KPI/ KRI reporting
- Oversight of incidents, vulnerabilities, and compliance findings
- Reviews of system onboarding decisions and risk acceptances
- Verification that roles such as Information Owners and System Owners are assigned and active
- Annual review of Business Continuity and Disaster Recovery test results, including verification that corrective actions have been implemented.

If non-adherence is identified:

- The deviation is documented and assessed as a risk or non-conformity
- Corrective actions are defined and assigned to responsible management
- Follow-up takes place to ensure timely resolution
- Significant or structural deviations are escalated to senior management

Where necessary, exceptions may only be accepted through formal risk acceptance with clear management accountability and documentation.

Monitoring outcomes are used to support continuous improvement of the ISMS and to ensure that the policy remains effective, relevant, and aligned with the organization's risk profile.

3.1.4 Enforcement

Violations of this policy may result in corrective measures, contractual action, or disciplinary consequences. Where necessary we will inform our external regulator.

NEON NL

Nucleaire Energie Organisatie Nederland

Nucleaire Energie Organisatie Nederland
Carel van Bylandtlaan 5
2596 HP, The Hague
The Netherlands
www.neonl.com
info@neonl.com