Data Classification & Information Protection policy

Nuclear Energy Organization Netherlands

Version:	[0.3]
Date:	[20 Januari 2026]
Workstream:	[IM/IT]
Owner:	[
Unique ID:	[2025.NNB.WS##.###.V1]

Content

A. Document management

Version	Date	Role	Changes
Concept 0.1	*Januari 19th 2026*	*Enterprise Architect*	*Made concept*
Concept 0.2	*Januari 20th 2026*	*CISO*	*Reviewed concept*
Concept 0.3	*Januari 21st 2026*	*Enterprise Architect*	*Reviewed concept*
Definitive 1.0		*Workstream lead owner scope*	*Finalized document*
Improved 1.2	April 19th 2026	CISO	Added IAEA compliancy and handling vendor information

Describe the input and people that worked to finalize this document. An example is provided above.

Revision and evaluation

- *Annual review for relevance*
- *Mandatory revision at least every 3 years or after major incidents or regulatory change*

Please revise by making text suggestions. Also, if you make a comment, please also suggest an improvement.

B. Introduction

1. Introduction

NEO NL is in a build-up phase and is preparing for the development and delivery of a nuclear power plant. The programme will operate under significant political attention and parliamentary oversight and will involve close cooperation with regulators, government bodies, and a wide range of suppliers

2. Context

In this environment, demonstrable and auditable control over information security and risk management is essential to maintain regulatory confidence, enable licensing, protect sensitive information, and support safe and reliable project execution. ISO/IEC 27001:2022 is the internationally recognised standard for information security management and is widely applied within the energy and nuclear sectors, providing the primary framework for NEO NL's information security governance.

In addition, ISO 19443 provides nuclear-sector-specific quality management requirements aligned with ISO 9001, supporting nuclear safety culture and supply chain assurance. Dutch national security regulations, including the VIR-BI (Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie), apply where State Secret information is handled.

Regulatory and contractual requirements imposed by the Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) take precedence where they impose stricter controls than internal standards.

3. Objectives and Scope

Objectives

This policy defines mandatory requirements for the classification, protection, handling, sharing, retention, and disposal of information relevant to nuclear safety, nuclear security, safeguards, emergency preparedness, and business operations.

The objectives are to:

- Ensure confidentiality, integrity, and availability of information throughout its lifecycle.
- Prevent unauthorised disclosure, alteration, or loss of sensitive information.
- Support compliance with legal, regulatory, licence, and contractual obligations.
- Enable effective cooperation with regulators and suppliers while protecting sensitive assets.

This policy supports NEO NL's ambition to achieve capability maturity level 3 (defined and measured) on a five-level scale, meaning that controls are consistently implemented and their effectiveness is monitored and demonstrable.

Scope

This policy applies to:

- All NEO NL employees, contractors, secondees, and interns.
- All third parties processing NEO NL information on its behalf.
- All forms of information, regardless of medium (digital, paper, verbal, physical) and location.

4. Information Classification Framework

NEO NL Classification Levels

NEO NL uses the following internal classification levels:

NEO NL Level	Description
Neo-Unclassified	Public or non-sensitive internal information
Neo-Internal	Routine business information not for public release
Neo-Restricted	Sensitive business, technical, or security information
Neo-Confidential	Very sensitive information affecting safety, security, or safeguards
Neo-Secret	Highly sensitive information affecting safety, security, or safeguards

5. Mapping to National and International Schemes

Where information is classified as State Secret, handling shall fully comply with Dutch law (VIR-BI) and issuing authority requirements.

Where we handle or receive information which is classified as a state secret, we will follow all the necessary rules and regulation about the handling of this information as described in the VIR-bi (Dutch Government Information Security Regulation (VIR-BI: Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie. Hyperlink in footnote)[1]

For clarification purposes the NEO NL classification scheme is compared to the Dutch Government and NATO in the matrix underneath.

NEO NL	BIO2	Dutch State Secret categories	NATO
Unclassified	Openbaar	Ongerubriceerd	UNCLASSIFIED
Internal	Intern		
Restricted	Vertrouwelijk	Departementaal VERTROUWELIJK (Dep.V.)	NATO RESTRICTED
Confidential	Confidentieel	Staatsgeheim CONFIDENTIEEL (Stg.C)	NATO CONFIDENTIAL
Secret	Geheim	Staatsgeheim GEHEIM (Stg.G)	NATO SECRET
Not Applicable for Neo	Zeer geheim	Staatsgeheim ZEER GEHEIM (Stg.ZG)	NATO TOP SECRET

[1] VIR-bi 2013, 15497

6. Roles and Responsibilities

Executive Management

- Ultimate accountability for information risk.
- Approval of risk acceptance exceeding defined thresholds.

CISO

- Policy ownership and governance.
- Risk management oversight.
- Regulatory and audit liaison.

Information Owners

- Assign classification and retention period as prescribed (by NEO, ANVS, IAEA).
- Approve access, declassification, and destruction.
- Ensure compliance with licence and policy requirements.
- Report periodically on compliance.
- Ensure employees and other associates know their information security requirements.

Users

- Handle information strictly according to classification and procedures.
- Report incidents or suspected breaches immediately.

7. Mandatory Protection Principles

- The control of our data should be clear based on The EU Cloud Sovereignty Framework SEAL
- Data is to be hosted in the EU subject to EU laws unless there is an explicit reason to accept this risk. (SEAL 2: Data Sovereignty is the minimal required level)
- Protection of information shall support nuclear safety and nuclear security in accordance with licence conditions.
- Risk-based controls are determined using ISO/IEC 27001 risk assessment methodology, with licence and legal requirements taking precedence were stricter.
- Access is granted strictly on a need-to-know and least-privilege basis.
- Defence-in-depth is applied across organisational, procedural, physical, and technical layers.
- Security responsibilities are integrated into business processes and supplier arrangements.

8. Protection Measures (ISO/IEC 27001 Aligned)

For Internal, Restricted and higher classifications, controls shall at minimum cover:

- Identity and access management with strong authentication (multi-factor).
- Zero Trust, Zero footprint, Security by Design and Default.
- Individual access authorisation and logging.
- Encryption for storage and transmission where applicable.
- Segregation of Information Technology (IT) and Operational Technology (OT).
- Continuous monitoring and incident detection.

For Confidential and Secret information, additional measures apply:

- The control of our data should be clear based on The EU Cloud sovereignty Framework SEAL
- Enhanced audit trails and management oversight.

For Secret information, additional measures apply:

- Full digital sovereignty is required (SEAL 4).
- Dual control (four-eyes principle).
- Segregated or dedicated processing environments.
- Compliance with national security authority requirements.

Detailed technical and procedural controls are specified in subordinate standards and procedures.

9. Third Parties, EPCs, and Suppliers

- Access is explicitly authorised, time-bound, and auditable.
- Information sharing is limited to what is strictly necessary.
- Contracts shall include:
    - Security requirements equivalent to NEO NL controls.
    - Right-to-audit clauses.
    - Mandatory incident notification.
    - Flow-down of requirements to subcontractors.

10. Lifecycle Protection

Information protection requirements apply throughout the full lifecycle, including creation, storage, use, transmission, archival, and secure destruction, consistent with licence conditions and long-term nuclear asset obligations.

11. Incident Reporting and Response

- Any actual or suspected compromise of Restricted or higher classified information shall be reported immediately to Security Operations and the Information Owner.
- Incidents shall be escalated to the CISO and external authorities where legally required.
- Incident handling follows ISO/IEC 27001-aligned response procedures and licence obligations.

12. Oversight and Compliance

- Compliance is subject to internal assurance, independent audits, and inspection by ANVS.
- Non-compliance may result in disciplinary, contractual, or legal action.

13. Handling Matrices and Operational Controls

Detailed handling requirements for physical security, logical access, transport, personnel vetting, and lifecycle controls are defined in subordinate standards and procedures, including:

- Personnel Security Standard
- Physical Security Standard
- ICT Security Baseline
- Classified Transport Procedure

14. Handling of Third-Party and Vendor Confidential Information

Purpose
This section defines the mandatory requirements for handling confidential and sensitive information received from third parties, including nuclear vendors, EPC (Engineering, Procurement, and Construction) contractors, and strategic suppliers. The objective is to ensure that such information is protected in accordance with the expectations of the originating party and applicable legal, contractual, and regulatory requirements.

Scope
This section applies to all NEO NL employees, contractors, and third parties who receive, access, process, store, transmit, or otherwise handle information originating from external parties.

Originator Control
Information received from third parties shall remain subject to the classification, handling instructions, and restrictions defined by the originating party.

- NEO NL shall not reclassify, downgrade, or alter the classification of such information without explicit written approval from the originator.
- Any limitations on use, distribution, or retention imposed by the originator shall be strictly followed.
- Where contractual agreements (e.g. NDA, EPC contracts) define additional requirements, these shall take precedence where stricter.

Access Control and Need-to-Know
Access to third-party information shall be restricted to individuals who require such access for the performance of their duties.

- Access shall be granted on a strict need-to-know and least-privilege basis.
- Information Owners are responsible for approving and periodically reviewing access rights.
- Personnel handling highly sensitive vendor information may be subject to additional screening or clearance requirements where applicable.

Controlled Use and Internal Sharing
Third-party information shall only be used for the purpose for which it was provided.

- Internal sharing within NEO NL shall be limited to what is strictly necessary for project execution or regulatory obligations.
- Information shall not be copied, reproduced, or redistributed beyond the defined scope without authorization.
- Where required, usage restrictions (e.g. “originator controlled” or “no further distribution”) shall be explicitly respected.

External Sharing and Disclosure
Third-party information shall not be disclosed to external parties without prior authorization.

- Any onward sharing with subcontractors, partners, or advisors requires approval from both the NEO NL Information Owner and, where applicable, the originating party.
- Disclosure in public domains (including presentations, reports, publications, or media interactions) is strictly prohibited unless formally approved.
- Legal, regulatory, or governmental disclosure obligations shall be coordinated with Legal, the CISO, and the originating party where possible.

Identification of Sensitive Vendor Information
Personnel shall treat third-party information as sensitive where it relates to, or may reveal:

- Design, engineering, or technical specifications of nuclear or critical infrastructure.
- Safety, security, or safeguarding systems and measures.
- Vulnerabilities, risk assessments, or incident information.
- Facility layouts, system configurations, or operational processes.
- Any information explicitly marked or reasonably understood to be confidential.

In case of doubt, the information shall be handled at the higher classification level.

Protection Measures
Third-party information shall be protected in accordance with its classification level and at least equivalent to NEO NL internal requirements.

- Storage, transmission, and processing shall follow the applicable controls defined in this policy and supporting standards.
- Where the originating party requires specific technical or organisational measures, these shall be implemented accordingly.
- Information shall be stored only in approved environments that meet required security and sovereignty levels.

Traceability and Accountability
NEO NL shall maintain appropriate records to ensure traceability of third-party information.

- Access, distribution, and key handling actions shall be logged where required by classification level.
- Copies of highly sensitive information shall be limited, uniquely identifiable where applicable, and controlled.
- Information Owners are responsible for maintaining oversight of information flows.

Incident Management
Any actual or suspected loss, unauthorized disclosure, or compromise of third-party information shall be reported immediately.

- Incidents shall be escalated to the responsible manager and the CISO and handled in accordance with the incident response process.
- Where required by contract or regulation, the originating party shall be notified without undue delay.

Retention and Disposal
Third-party information shall be retained only as long as necessary and in accordance with contractual and regulatory obligations.

- Upon completion of its purpose, information shall be securely archived, returned, or destroyed as agreed with the originating party.
- Destruction shall be performed in a manner that prevents reconstruction or recovery of the information.

Compliance and Assurance
Compliance with this section is mandatory.

- NEO NL reserves the right to audit compliance internally and, where applicable, support audits by originating parties or regulators.
- Non-compliance may result in disciplinary measures, contractual consequences, and legal action.

The matrices underneath operationalize the requirements of this policy. They are mandatory for all applicable parties.

C. Consolidated Matrices of Handling Instructions

The 'V' signifies that the measure is applicable in the various information classifications.
The classification Top Secret is not used by NEO. Top Secret is a government classification.

Register of owners and handlers

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Register all assets and the persons to whom they have been issued.			V	V
B	Register the location/base of all assets and their assignment to an owner.			V	V

Persons handling classified information

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Persons who deal with classified information must sign a confidentiality agreement. This also records that, after the role ends, the person remains bound by that duty of confidentiality.	V	V	V	V
B	Persons who frequently deal with classified information must also hold an appropriate certificate/clearance.	VOG1	VGB-C	VGB-B	VGB-A
C	When a role ends in which someone encounters classified information, it is ensured that the person no longer has access to that information and does not have it in his/her possession.	V	V	V	V

Physical/ environmental requirements

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Classified information is handled and stored in such a way that there is a positive security return1, based on damage acceptance and the threat profile.	V	V	V	V
B	TEMPEST measures in accordance with the Policy Advice on Compromising Emanations (VBV 32000).		V	V	V
C	Prevent eavesdropping and prevent visibility of, and reflection of, information (e.g. via display screens or reflective surfaces).		V	V	V
D	The employee responsible for processing classified information must ensure that visitors cannot become aware of the classified information under his control.	V	V	V	V
E	Visitors are escorted when they enter rooms where classified information is present.		V	V	V
F	Visitors are registered if they (may) have access to classified information in the rooms they enter, where access to that information cannot be prevented in another way (e.g. cabinet/safe, etc.).			V	V

Logical access controls

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Access to an account is blocked after a number of consecutive incorrect login attempts.	5	3	3	3
B	Access to systems may be determined at group level.	V	V	V	not permitted
C	Access to classified information is determined at an individual level.			V	V

Life cycle management

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Throughout the entire life cycle of a system, periodic audits, inspections, reviews and tests are carried out to verify that the security measures are effective. These checks are performed by specialist experts who have the right investigative tools and proven methods.	Self-assessment	Self-assessment	Independent expert	Independent expert
B	Responsibilities and procedures for proper management and correct use of the ICT facilities in which classified information is processed have been defined.	V	V	V	V
C	For the management of ICT facilities, the security level is aligned with the risks.	V	V	V	V
D	When (parts of) service provision are outsourced, the same security level must be achieved as applies to internal service provision.	V	V	V	V

Transmission of confidential information

	Measures	Internal or Restricted	Confidential	Secret	Top Secret
A	Digital transmission of classified information must be carried out using cryptographic means approved by the Ministry. Ministerial approval is granted on the basis of advice from the Working Group for Classified Information Security (WBI) or its successor on the security strength of the cryptographic means.		V	V	V
B	Digital transmission of information obtained under an international treaty or international agreement must be sent using cryptographic means approved by the issuing authority.			V	V
C	Physical dispatch of classified information must be carried out using means approved by the Ministry, ensuring that the contents are not visible, not discernible and that tampering is detectable.	V	V	V	V
D	Physical dispatch is carried out by: An authorised employee, whereby the information remains under the carrier's control at all times and is not opened during transport. A Ministry-approved courier service. A military, government or diplomatic courier.		V	V	n/a
E	National dispatch exclusively via a government courier.				V
F	International dispatch exclusively as a diplomatic courier shipment or military transport.				V
G	For both digital and non-digital delivery, there is irrefutable confirmation of receipt.		V	V	V
H	Security-relevant actions are logged/recorded.	V	V	V	V
I	The creation, updating, modification, retrieval, consultation, use, disclosure by forwarding, dissemination or any other form of making available, and the destruction of classified information are recorded.			V	V

J	At a minimum, each document must, upon distribution, state: Classification level; Classification duration; Page numbering and the total number of pages in the document;	V	V	V	V
K	Each document is provided with: Copy number.		V	V	V
L	For all copies of classified documents, the following details are recorded: Copy number; Creator; Recipient.		V	V	V
M	No more copies of classified information are made than is strictly necessary.		V	V	V

D. European Commission Cloud Sovereignty Framework

Below the detailed list of Sovereignty Effectiveness Assurance Levels (SEAL) defined:

Sovereignty Effectiveness Assurance Levels	Sovereignty Effectiveness Assurance Levels Descriptions
SEAL-0	No Sovereignty: Service, technology or operations under exclusive control of non-EU third parties, governed entirely in non-EU jurisdictions.
SEAL-1	Jurisdictional Sovereignty: EU law formally applies with limited practical enforceability; service, technology or operations under exclusive control of non-EU third parties.
SEAL-2	Data Sovereignty: EU law applicable and enforceable, with material non-EU dependencies remaining; service, technology or operations under indirect control of non-EU third parties.
SEAL-3	Digital Resilience: EU law applicable and enforceable, EU actors exercising meaningful but not full influence; service, technology or operations under marginal control of non-EU third parties.
SEAL-4	Full Digital Sovereignty: Technology and operations under complete EU control, subject only to EU law, with no critical non-EU dependencies