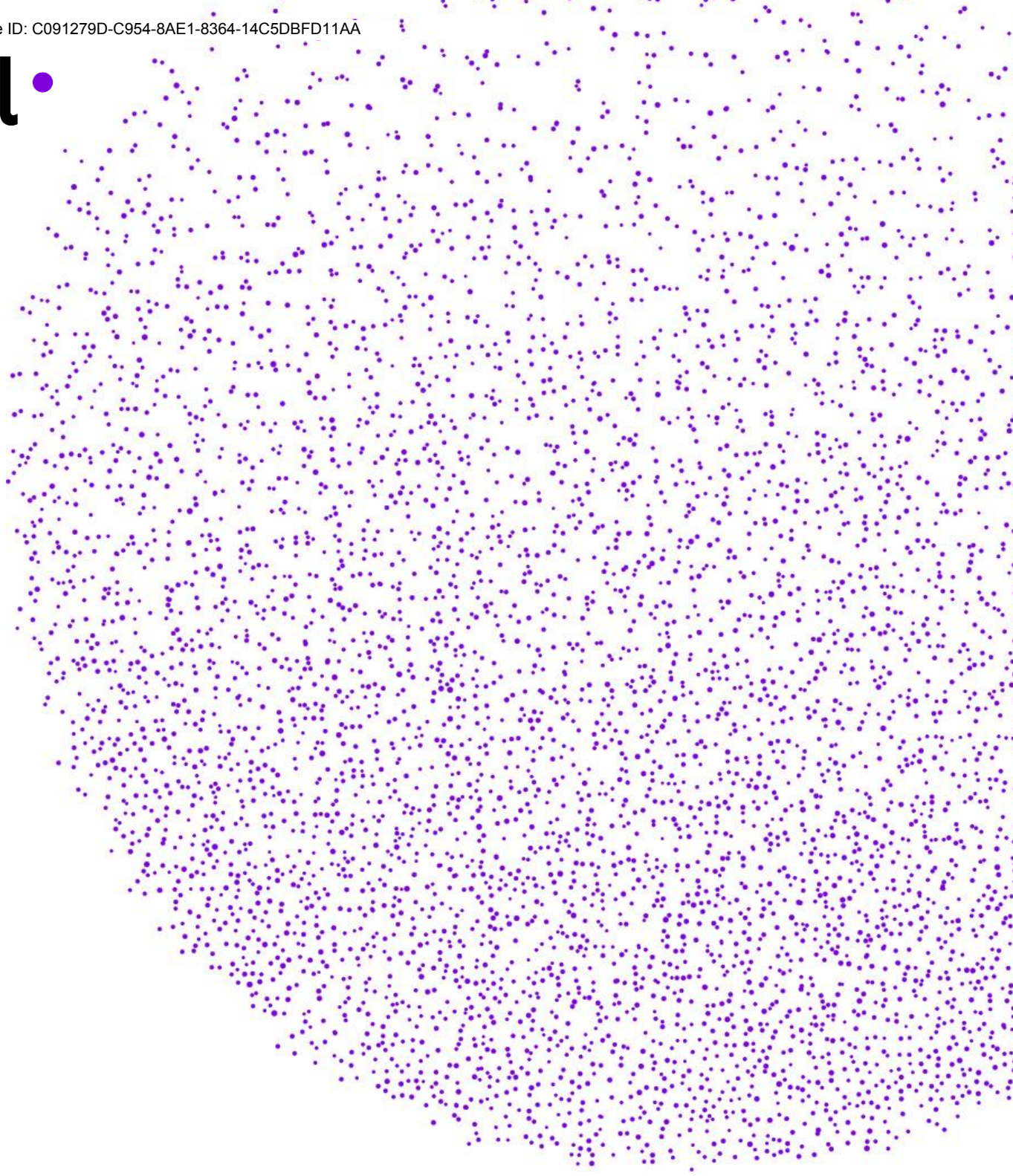
Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA



Information Security Policy for Nel ASA

Date: 2026-09-21

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Contents

Purpose 2
Who must Comply with the Policy? 2
Owner of the Policy 2
Chief Executive's Statement of Commitment 3
Introduction 4
Security Objectives 4
Information Security Policy Framework 5
Information Security Roles and Responsibilities 5
Monitoring 5
Legal and Contractual Obligations 5
Training and Awareness 6
Continual Improvement of the ISMS 6
Compliance Measurement 6
Exceptions 6
Non-Compliance 6

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Purpose

The purpose of the Information Security Policy is to establish a framework that guides an organization's approach to protecting its information assets. The policy serves as a foundational document that communicates the organization's commitment to information security and provides a set of principles, guidelines, and expectations for employees and stakeholders.

The Information Security Policy is an important part of Nel's security measures and describes the level of security approved by the Board of Directors.

Who must Comply with the Policy?

This Information Security Policy (the "**Policy**") applies to Nel ASA and its subsidiaries where Nel ASA, directly or indirectly effectively controls 50 % or more of the shares and votes in the entity in question (hereinafter jointly "**Nel**"), including all Nel's directors, officers, employees, and hired-in personnel whether full-time, part-time, permanent, or temporary (including hired-in-personnel), (the "**Employees**").

We expect all our business partners to also comply with the Policy, including but not limited to anyone with whom we do business, i.e., suppliers, customers, distributors, agents, intermediaries, resellers, consultants, contractors, associates, lobbyists, joint venture partners or other third parties who are acting on behalf of Nel ("**Business Partner(s)**"). Business Partners such as agents and other third-party intermediaries who are acting on behalf of and/or representing Nel will hereinafter be referred to as "**Representatives**". The Policy also applies to the members of the Board of Directors of Nel ASA. We expect Nel, the Employees, Board of Directors and all our Business Partners to comply with applicable laws, rules and regulations, as well as internationally accepted guidelines, conventions or similar normative documents relating to information security (jointly referred to as the "Applicable Rules"), as well as the specific requirements in the Policy and other applicable Policies and Procedures.

Owner of the Policy

The Board of Directors of Nel ASA is the owner and approver of this Policy. Global IT is the functional owner and is responsible for the maintenance, communication and monitoring of the Policy, including implementing any necessary changes.

Any exceptions from the Policy shall be approved by the CEO of Nel ASA, acting as data-controller in writing.

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Chief Executive's Statement of Commitment

I, Håkon Volldal, as the Chief Executive Officer of NEL ASA, hereby commit to the following:

- I will ensure that the organization has an effective information security management system (ISMS) in place.
- I will provide the necessary resources to support the implementation and maintenance of the ISMS.
- I will promote a culture of information security awareness and responsibility throughout the organization.
- I will hold all employees accountable for complying with the ISMS.

I will keep the Board of Directors appraised of material developments, deviations, and events related to the information security policy framework. I am aware that the effective protection of our information assets is essential to the success of our organization. I am committed to ensuring that we have in place the necessary controls to protect our information from unauthorized access, use, disclosure, modification, or destruction.

I am aware that the security of Nel and its customers' information assets depends on having critical suppliers maintaining or exceeding the security standards of Nel. I am committed to ensuring that the critical suppliers for Nel's production and products undergo proper screening, and that the supply chain risk management is an ongoing and effective security measure at Nel.

This commitment is made on behalf of the entire organization and will be reviewed and updated on a regular basis to ensure that it remains relevant and effective.

Signed by:

7D31B9767A674B3...

Håkon Volldal, CEO

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Introduction

The effective protection of information assets is essential to the success of any organization. The purpose of this Policy is to establish Nels commitment to information security and to define the principles and controls that will be used to protect its information assets.

Nel's main source of revenue is manufacturing equipment, therefore special consideration is given to the manufacturing and support processes.

This Policy is based on the requirements of ISO 27001, the international standard for information security management systems. ISO 27001 provides a framework for organizations to manage their information security risks and to protect their information assets from unauthorized access, use, disclosure, modification, or destruction.

Security Objectives

Nel's security objectives are to:

- Assure the safety of its employees
- Protect the confidentiality, integrity, and availability of its information assets.
- Protect the information security of assets procured by its customers during development, construction, installation and during the asset life cycle.
- Protect customer data from unauthorized access, use, disclosure, modification, or destruction.
- Comply with all applicable laws and regulations related to information security.
- Raise awareness of information security among all employees and stakeholders.
- Protect the organization from damage caused by security breaches.
- Provide a structured approach to securing information.

Information Security is defined as preserving:

Confidentiality	Access to Information is to those with appropriate authority The Right Access
Integrity	Information is complete and accurate To the Right Data
Availability	Information is available when needed At the Right Time
Authentication	Verifying the identity of users and entities. To the Right People
Authorization	Granting appropriate access privileges to users At the Right Level

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Information Security Policy Framework

The Information Security Management System is built upon an Information Security Policy Framework. In conjunction with this policy, the following policies make up the Policy Framework:

- Information Security Policy: This policy.
- Data Protection Policy
- Acceptable use of Assets Policy
- Identity and Access Management Policy
- Incident Response and Recovery Policy
- Physical and Environmental Protection Policy
- Configuration Management Policy
- System Security Policy
- Enterprise Risk Management Policy
- Information Security Management System (ISMS)

Information Security Roles and Responsibilities

Information Security is the responsibility of everyone. All members of the scope of this policy are required to adhere to the policies, follow procedure and report suspected or actual breaches. Specific roles and responsibilities are detailed in the ISMS document.

Monitoring

Global Leadership team shall appoint a Chief Information Security Officer (CISO). Compliance with the policies and procedures outlined in the ISMS is conducted by the CISO, together with independent internal and external audits on a regular basis.

Legal and Contractual Obligations

Nel takes its Legal and contractual obligations seriously. Compliance to Laws, regulations and customer requirements are considered in the Nel Security Plan, Enterprise Risk Management Process, Change Management Process and Supplier Risk Management Process

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights

Docusign Envelope ID: C091279D-C954-8AE1-8364-14C5DBFD11AA

Training and Awareness

Policies are made easily accessible to all Employees and third parties. A training and dissemination plan is in place to communicate the policies, process, and concept of information security. Training needs are identified, and training requirements are captured as per the "Training Awareness Procedure".

Continual Improvement of the ISMS

The ISMS is continually improved. The improvement process takes input from the Security Risk Management Process, the yearly review, and input from external auditors.

Compliance Measurement

All controls stated in the ISMS shall be measured for effectiveness by an external auditor on an ongoing basis.

Exceptions

All requests for exceptions or changes to this policy shall be directed at the Nel ASA acting CISO, who will act as secretary for CEO/BoD approval.

Non-Compliance

Violations of this policy may result in disciplinary action, according to what is possible given the local rules and legislation. The Business Unit may also take legal action against violators.

Nel proprietary. This document and its accompanying elements contain information which is proprietary and confidential and the property of Nel ASA and/or its affiliates. Any disclosure, copying, distribution or use is prohibited if not otherwise explicitly agreed with Nel in writing. Any authorized reproduction, in whole or in part, must include this legend. © 2010-2026 Nel – All rights