
	Issue number 7	Document number PO10003	Classification	Page 1 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

## Content Table

<b>1</b>	<b>PURPOSE</b> .....	<b>2</b>
<b>2</b>	<b>SCOPE</b> .....	<b>2</b>
<b>3</b>	<b>DEFINITIONS AND ABBREVIATIONS</b> .....	<b>2</b>
<b>4</b>	<b>ROLES AND RESPONSIBILITIES</b> .....	<b>2</b>
<b>5</b>	<b>REFERENCES AND RELATED DOCUMENTS</b> .....	<b>2</b>
<b>6</b>	<b>FORMS</b> .....	<b>3</b>
<b>7</b>	<b>RECORDS</b> .....	<b>4</b>
<b>8</b>	<b>ENVIRONMENTAL</b> .....	<b>4</b>
<b>9</b>	<b>INFORMATION SECURITY</b> .....	<b>4</b>
<b>10</b>	<b>HEALTH &amp; SAFETY</b> .....	<b>4</b>
<b>11</b>	<b>POLICY</b> .....	<b>4</b>
11.1	OBJECTIVES .....	4
11.2	POLICY STATEMENT.....	4
11.3	COMPLIANCE .....	4
11.4	CONTINUAL IMPROVEMENT .....	5
<b>12</b>	<b>APPENDICES / ATTACHMENTS</b> .....	<b>6</b>
<b>13</b>	<b>DOCUMENT HISTORY</b> .....	<b>7</b>

	Issue number 7	Document number PO10003	Classification	Page 2 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

## 1 PURPOSE

This Information Security Policy aims to set high-level policies and principles for information security within Neuvén.

Information that is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss, and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, noncompliance with standards and legislation, as well as possible judgements against Neuvén.

Several other policies and procedure documents support this policy – see section 5 References and Related Documents below.

## 2 SCOPE

This policy and its supporting controls, processes and procedures apply to all information used at Neuvén, in all formats. This includes information processed by other organisations in their dealings with Neuvén.

This policy and its supporting controls, processes and procedures apply to all individuals accessing Neuvén information and technologies. This includes any external parties that provide information processing services to Neuvén.

## 3 DEFINITIONS AND ABBREVIATIONS

For further Definitions and Abbreviations please refer to the [Glossary](#)

Term/Abbreviation	Definition
GDPR	General Data Protection Regulation
DPA 2018	Data Protection Act

## 4 ROLES AND RESPONSIBILITIES


Information Security Manager

The Information Security Management Systems Manager at Neuvén is responsible for ensuring that the Integrated Management System conforms to the requirements of ISO 27001:2022. They also report on the performance of the system to top management concerning security.

NOTE: the Activities detailed in this document align with the Roles and Responsibilities in the above table.

## 5 REFERENCES AND RELATED DOCUMENTS


Doc No	Document Title
<a href="#">IM00001</a>	Integrated Management System Manual
ISO27001:2022	Information Management System Requirements

	Issue number 7	Document number PO10003	Classification	Page 3 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

<a href="#">PO12000</a>	Personal Data Breach Policy
<a href="#">PO12001</a>	End User IT, Communications, Security and Monitoring Policy
<a href="#">PO12002</a>	Social Media Policy
<a href="#">PO12002</a>	Information Transfer Policy
<a href="#">PO12003</a>	User Access Control Policy
<a href="#">PR16000</a>	Returning a Company Mobile
<a href="#">PR16001</a>	Company Mobile Phone Setup Guide
<a href="#">PR16002</a>	Business Continuity and Disaster Policy
<a href="#">PR16003</a>	Information Security Risk Management Procedure
<a href="#">PR16005</a>	Incident Response Procedure
<a href="#">PR16006</a>	Vulnerability Management Procedure
<a href="#">PR16007</a>	Configuration Management Procedure
<a href="#">PR16008</a>	Secure Development Lifecycle
<a href="#">PR16009</a>	Secure Coding Practices
<a href="#">PR16010</a>	Contact with Authorities Procedure
<a href="#">PR16011</a>	Contact with Special Interest Groups Procedure
<a href="#">PR16012</a>	Software Change Management Procedure
<a href="#">PR16004</a>	Software Testing Policy & Procedure
<a href="#">PO11009</a>	Homeworking Policy
<a href="#">PO11015</a>	Disciplinary Policy and Procedure
<a href="#">PO11023</a>	Training and Development Policy
<a href="#">PO13002</a>	Improvement Procedure

## 6 FORMS

NOT APPLICABLE

	Issue number 7	Document number PO10003	Classification	Page 4 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

## 7 RECORDS

NOT APPLICABLE

## 8 ENVIRONMENTAL

There is no direct environmental consideration for this policy.

## 9 INFORMATION SECURITY

This Policy is written to support the requirements of ISO27001:2022

## 10 HEALTH & SAFETY

There is no direct Health and Safety consideration for this policy.

## 11 POLICY

### 11.1 Objectives

Neuven's security objectives are as follows:

- Information risks are identified, managed and treated according to the documented risk tolerance in [PR16003 Information Security Risk Management Procedure](#).
- Authorised users can securely access and share information in order to perform their roles.
- All physical, procedural, and technical controls will balance the business needs and security.
- All contractual and legal requirements relating to information security will be met.
- Individuals accessing our information are aware of their information security responsibilities.
- Incidents affecting our information assets are resolved in line with [PR16005 Incident Response Procedure](#).

### 11.2 Policy Statement

It is Neuven's policy to ensure that information is protected from loss of:

- Confidentiality – information will be accessible to authorised individuals.
- Integrity – the accuracy and completeness of information will be maintained.
- Availability - information will be accessible to authorised users and processes when required.

Neuven will implement an integrated management system that supports all certified standards as required. Neuven will be mindful of the approaches adopted by its stakeholders.

Neuven will adopt a risk-based approach to all controls identified in its policies and procedures.

### 11.3 Compliance


The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes:

- Data protection legislation
- Neuven's contractual commitments

Neuven will use a combination of internal and external audits to demonstrate compliance against ISO 27001:2022 and best practices.

Failure to comply with the information management system could result in disciplinary actions.


	Issue number 7	Document number PO10003	Classification	Page 5 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

#### 11.4 Continual Improvement

Neuven is committed to continual improvement and will use inputs from a variety of sources to determine appropriate improvements including but not limited to:


- Internal audit findings
- External audit findings
- Customer feedback
- Employee feedback
- Identified risks and opportunities
- Incidents

All improvements will be managed following [PO13002 Improvement Procedure](#)

	Issue number 7	Document number PO10003	Classification	Page 6 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

**12 APPENDICES / ATTACHMENTS**

NOT APPLICABLE

	Issue number 7	Document number PO10003	Classification	Page 7 OF 7
Document owner	Chief Technology Officer	Approved By	Board Directors	
TITLE:	Information Security Policy			

### 13 DOCUMENT HISTORY

Version:	5	Originator(s):	CTO
<b>Summary of Change:</b>	Rewritten to align with base expectations and updated to new format.		
Version:	6	Originator:	IMS Representative
<b>Summary of Change:</b>	Updated font / Sent for approval on ISMS		
Version:	7	Originator:	CTO
<b>Summary of Change:</b>	Updated to add clarity to objectives, related documents, compliance and continual improvement		