# INFORMATION SECURITY POLICY

Oy Lining Ab

Ismo Nieminen
ismo.nieminen@lining.fi

Lining
INDUTRADE GROUP

Validity and version history

| Version history | | | | |
|---|---|---|---|---|
| Date | Version | Author | Description of changes | Approved by |
| 13.6.2023 | 0.9 | Ismo Nieminen | First version of the document | |
| 26.6.2023 | 1.0 | Ismo Nieminen | Approved version | Pasi Mönkäre |
| 18.1.2024 | 1.0EN | Ismo Nieminen | English translation | Pasi Mönkäre |
| | | | | |

# Table of Contents

# 1. Introduction

The business operations of Oy Lining Ab are guided by the Operations Manual, which combines the company's quality, sustainability, and information security guidelines. The information security goals, strategy, responsibilities, and roles are outlined in Oy Lining Ab's Information Security Policy.

In its operations Lining utilizes centralized ICT support services provided by the parent company Indutrade Oy. In cases where the Information Security Policy of Lining does not describe a particular function, the Information Security Policy, and Guidelines of Indutrade Oy are followed.

This document is intended for all employees and business partners of Oy Lining Ab and will be applied in all of Lining's operations.

# 2. Objective of the Information Security Policy

The objective of the Information Security Policy is to protect Oy Lining Ab, its personnel, assets, and information, as well as to ensure the continuity of operations. The information security policy serves as the foundation for the operating environment in which the security of information systems, data, and data processing can be assured.

# 3. Methods

The following paragraphs describe the general methods for information security management used by Oy Lining Ab. More detailed descriptions and actions are outlined in the company's Operations Manual and internal process descriptions.

## 3.1. Identification of Risks and Threats

Information security is considered in all aspects of Lining's operations. Special attention is given to threats and risks related to information systems and personnel. Lining's operating environment is continuously monitored to identify cyber threats and risks.

The Information Security Working Group, led by the Information Security Manager, is responsible for managing information security risks. The urgency of required actions is calculated based on a formula from threats and risks. Risks and threats are documented and regularly reviewed.

Enterprise Risk Management (ERM) processes are employed in business risk management, and their operation is detailed in the Operations Manual.

## 3.2. Implementation

The guidelines for implementing information security are the Operations Manual and the Information Security Policy. These documents outline the practices and methods through which Lining ensures its information security.

### 3.2.1. Access control

Access rights and access control at Lining adhere to the principle of least privilege. Employees, collaborators, devices, applications, or technologies should have only the minimum necessary permissions to access resources managed by the company, ensuring efficient and secure business operations. The principle of least privilege is also followed in access control for physical premises.

### 3.2.2. Data classification

Files stored in information systems are classified based on their sensitivity. The handling and transfer of classified data are automatically monitored to prevent unintentional or intentional dissemination of classified information. It is the responsibility of the employee to assign the appropriate classification to the information they produce.

### 3.2.3. Employee Training

An orientation program that includes the use of an orientation checklist for monitoring is utilized. The orientation also includes information security guidance. The orientation program is primarily intended to guide new employees, but it can also be used in cases where an existing employee changes roles within the company.

Training must be continuous, meaning that as the operating environment changes, employees are briefed on the changes and trained if necessary. Incidents or predicted exceptional situations, as well as near-miss situations regarding information security, are considered topics for additional training.

Employees receive annual training on information security.

### 3.2.4. Recovery and Business Continuity Processes

Lining's business continuity and recovery processes are documented, practiced, and reviewed periodically. The data center and server solutions used by the company must be redundant and meet the data center and equipment space requirements set by Lining and the Indutrade group's ICT management.

## 3.3. Partners

The level of information security of Lining's business partners is assessed based on information provided by each partner. A partner must meet the quality and security criteria set by Lining. Compliance with partner requirements is continuously monitored, and the rights and privileges granted to partners are supervised. The granted privileges have a validity period.

Supplier audits may also be conducted on partners as needed to ensure compliance with service and operator requirements.

## 3.4. Continous Improvement

Continuous improvement is an essential part of Lining's strategy and operational activities. It can be initiated through various means, including:

- Metrics, key performance indicators, customer feedback, and analysis data
- Utilizing observations from internal and external audits
- Addressing product and service needs initiated by the Management Team
- Initiatives and ideas
- Detected incidents or threats

## 3.5. Incident and Risk Management

Lining continuously develops its processes to improve its operations and information security. The company undergoes regular internal and external audits based on information security, quality, environmental, and sustainability metrics.

Risk management follows Oy Lining Ab's Enterprise Risk Management (ERM) process, as described in the operational manual. Root causes of incidents are investigated in collaboration with the business, and corrective actions are taken if improvement areas are identified.

### 3.6. Device Management Policy

Lining utilizes centrally managed computers and mobile devices. Devices are locked at the operating system level into the device management system, preventing unauthorized device usage without valid company user credentials.

Device management policies enforce an adequate level of information security on the devices, and the installation of applications can be monitored and restricted. Device storage is encrypted, and devices are configured to install updates automatically. The security monitoring of the devices is automated. The company's communication or collaboration applications cannot be used on mobile devices unless the device is compliant with the settings required by mobile device management.

The current device management policy is outlined in the Operations Manual.

## 4. Personnel

Lining's personnel management utilizes the use of In, Transfer, and Exit processes, overseen by the supervisor. Onboarding of personnel is guided by an up-to-date orientation plan. Access rights granted to personnel are regularly reviewed and adjusted whenever job responsibilities change. New orientation according to the orientation plan is conducted when an individual's job responsibilities change.

Upon termination of employment, the Exit process is implemented, during which the individual's responsibilities and duties are transferred to the successor or supervisor. Granted access rights and privileges are revoked, and tools and devices used by the individual are returned and handled according to the ICT process.

The qualification requirements for personnel are outlined in the Operations Manual, and as needed, Lining provides training tailored to job responsibilities. As a company, Lining encourages the continuous education and development of its personnel. The activities of the personnel are guided by the Indutrade Group's Code of Conduct.

## 5. Responsibilities and Organization

Information security management is part of the company's overall leadership and is ultimately the responsibility of the CEO. The CEO owns the Information Security Policy, as well as the Integrated Management System and the Information Security Management System.

The management of information security activities and their supervision are led by the Information Security Manager. The Information Security Manager also serves as the lead for the Information Security working group and is the owner of the ISO 27001 certification.

Every employee and partner of Oy Lining Ab is responsible for information security in their respective roles. Personal and role-specific responsibilities and authorities, as well as monitoring, reviews, and meeting practices, are outlined in the Operations Manual.

### 5.1. Management Team Meetings

Lining's Management Team meetings are held at least five times per year. Participants include members of the senior management and business managers. In quality and information security matters the meeting may include additional experts as needed.

Agenda items include financial and personnel-related matters, operational activities of the business, as well as the implementation and monitoring of goals set by the Management Team.

## 5.2. Management Reviews

Management reviews are conducted as needed, but at least once per year. The review may cover topics such as incidents, audits, processes, changes in the operating environment, as well as an analysis of risks and opportunities. The management review involves the quality manager and the Management Team supplemented by experts if necessary.