Group Policy

Loomis – Group Information Security Policy

Document information		
Document type	Group Policy	
Adopted by / date	Board of Directors	2025 – 01 – 09
Document number		
Governance area owner	CEO	
Functional document owner	CISO	
Next review	2026	
Confidentiality	Open internally / Open externally	

Contents

1. **Introduction** 3

 1.1. Background and purpose 3

 1.2. Scope 3

 1.3. Structure of related documents 3

2. **Roles and responsibilities** 3

3. **Information security strategy** 4

4. **Security awareness** 5

5. **Exemptions and deviations** 5

6. **Update and approval** 5

7. **Contact person** 5

Appendix 6

1. Introduction

1.1. Background and purpose

Loomis AB ("**Loomis AB**" and together with its subsidiaries the "**Group**") has issued this document to form the Group's Information Security Policy (the "**Policy**").

The Policy aims to provide an overa

rching framework, a commitment of undertaking, to apply information security controls throughout the Group. Information security is the safeguarding of all type of information and information resources within the Group. The digital aspects of information security is considered IT security.

The objective of the Group's work with information security is to safeguard the confidentiality, integrity, availability, and traceability of the Group's information and information resources. These terms are defined in the Appendix.

The information security controls can be both technical, administrative and physical, and need to ensure a high level of traceability for compliance.

1.2. Scope

This Policy applies to all legal entities within the Group and their respective employees and consultants.

1.3. Structure of related documents

The Group's governance documents related to this Policy consist of a CEO instruction with related controls and references. Those are also reflected in the ICRs (Internal Control Requirements) regarding Information and IT-security controls.

In addition to the above, local governance documents may be implemented in accordance with what is set out in Section **Error! Reference source not found.** below.

Dependent upon the subject matter, the governance documents relating to this Policy will apply either globally or to specific companies or individuals within the Group. Employees, who have access to Loomis's computers, information systems or key information, and any other parties who have been granted such access, are responsible for complying with the governance documents that are applicable to them.

2. Roles and responsibilities

Loomis AB's CFO (Chief Financial Officer) has the overall responsibility to oversee implementation of this Policy in the Group and to secure that it is monitored and that the result of such monitoring is reported to the Board of Directors. Monitoring should also include supplier relations regarding ICT arrangements.

Each Country President is responsible for ensuring that this Policy is implemented in its respective country and that such country's handling of information follows this Policy and applicable local laws and regulations. This also applies in relation to information managed in shared or global systems.

Loomis AB's CFO may, on a case by case basis, resolve that with respect to a certain Group entity such entity's Chief Executive Officer, and not the Country President of the relevant country, shall carry the responsibilities set out in this Section **Error! Reference source not found.**. In such case, what is set out for the Country President in this Policy shall instead apply to such entity's Chief Executive Officer.

The Group CISO (Chief Information Security Officer) has the overall responsibility for the development and implementation of the group wide information security strategy which shall include policies, instructions and guidelines as part of the ISMS (Information Security Management System).

The Group CISO organization resides within Group IT and reports to Loomis AB's CFO with information security matters. IT-security related matters resides within Group IT.

The Country President is responsible for developing and implementing local supporting guidelines and instructions based on this Policy. Each department manager has the responsibility to support the Country President with appropriate instructions, to ensure that all services and information processes, owned by the department comply with information security requirements in regards to confidentiality, integrity, availability, and traceability. The Country President is also responsible to assign necessary roles and responsibilities to ensure that all information, irrespective of if in verbal or written form, is classified and handled with a consistent level of confidentiality, integrity, availability, and traceability.

All employees and consultants within the Loomis Group shall maintain a high level of security for information, based on business, contractual and regulatory requirements. Unauthorized disclosure of sensitive information as well as negligent operation of the Group's IT services and equipment in violation of applicable instructions could result in claims for damages and is considered as a material breach of the employment contract.

3. Information security strategy

The overall strategy for the Group's information security work is described in the Loomis Group Information Security Management System (ISMS) which shall be established in alignment with the ISO27001 standard and established regulatory requirements. The ISMS should also ensure digital operational resilience. The Group CISO is responsible for the lifecycle management of the ISMS. The ISMS shall enable entities in the Group to establish a baseline for information security in compliance with local regulations as well as support local ISMS if needed. Local ISMS shall as well be aligned with the ISO27001 standard.

4. Security awareness

Connected to the objectives, roles & responsibilities and steering documents as described in this Policy, a security awareness program should be running. The intention of the program is to strengthen the information security awareness for all employees and consultants within the Group. The program should be managed and monitored by Loomis AB as part of the ISMS with local support from country representatives. The program should as a minimum include:

- Security awareness training as part of Loomis Academy
- Phishing campaigns to ensure information security awareness in the handling of e-mail
- Security awareness material grouped per predefined functions in the Group

5. Exemptions and deviations

Any exemptions from this Policy shall be approved by the Board of Directors.

Any identified deviation from this Policy shall be reported to the Loomis Group CFO.

6. Update and approval

The Board of Directors shall review and adopt this Policy annually or, if deemed necessary, whenever there is a need or requirement to do so.

7. Contact person

If you have any questions about this Policy you may contact the Loomis Group CISO.

* * *

Appendix

Definitions

Availability is a property of being accessible and usable on demand by an authorized entity, ensuring that all information, including stored information and processing capability, are always available to authorised users when needed.

Confidentiality is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes, ensuring that information and processing capability are protected from unauthorised disclosure or use.

Information Security is the preservation of confidentiality, integrity, availability, and traceability of information.

Integrity is a property of accuracy and completeness, ensuring that all information is not subject to malicious or accidental alteration and that system processes function correctly and reliably.

Traceability The process of identifying, capturing and maintaining the records of all activities related to a particular event or transaction.

* *