Cyber Security and Compliance Framework Policy

Document information

Policy Owner	CIO
Document owner	CISO
Approved by	Board LiAB
Valid from:	2026-06-17
Revision date:	Latest 2028
Version:	1.0
Applies to	Lindab Group

Lindab Group

Contents

1. Foreword by the Board of Directors of Lindab International AB

At Lindab Group, cyber security and compliance is how we keep our customer promise and earn trust. It's the backbone of robust production, resilient supply chains and dependable deliveries; by treating our co-workers', customers' and partners' data securely and ethically, complying with laws and regulations, and making risk-aware decisions, we enable sustainable growth and our ambition to be Europe's leading ventilation company. This policy is our shared commitment, and each one of us makes it happen.

2. Purpose

This policy establishes Lindab Group's overarching requirements and principles for cyber security and compliance governance. It defines the foundation for how Lindab Group identifies, manages, and responds to cyber and information security risks across the organisation.

The purpose of this policy is to:

- Protect the confidentiality, integrity, and availability of Lindab Group's information assets, systems, and services.
- Define clear accountability and governance structures for cyber security and compliance across all levels of the organisation.
- Ensure compliance with applicable legal, regulatory, and contractual obligations.
- Provide a consistent and risk-based foundation for the Cyber Security and Compliance Framework and its supporting directives.

3. Scope

The policy applies to:

- All employees, consultants, temporary staff, and contractors of Lindab Group.
- All information assets, regardless of format (digital, physical, verbal), including Information Technology (IT), Operational Technology (OT), and all systems, applications, networks, and services owned or operated by Lindab Group.
- All third parties that access, process or manage Lindab's information.

This policy applies globally across all business units, legal entities, and geographies in which Lindab Group operates.

4. Exceptions

Lindab Group recognises that there may be circumstances where full compliance with this policy or its supporting directives is not immediately achievable. In such cases, a formal exception process must be followed to ensure that risks are understood, accepted, and actively managed.

All exception requests must include a written justification, a documented risk assessment, proposed compensating controls, and a defined end date. Exceptions must be approved by the CISO and equivalent authorised decision-maker prior to implementation. Exceptions with significant risk exposure must be escalated to the relevant management body.

All approved exceptions are time-limited, shall not exceed a maximum duration of 12 months, must be recorded in a central exception register, and reviewed at least annually. Where an exception cannot be resolved within the agreed timeframe, a new exception request must be submitted and re-approved. The assigned risk owner is accountable for ensuring compensating controls are maintained and that the exception is resolved within the agreed timeframe.

Failure to comply with this policy or its supporting directives without an approved exception may result in disciplinary action in accordance with applicable employment policies and procedures. For third parties, non-compliance may result in contractual remedies, including termination of the relevant agreement.

5. Principles

The following principles define Lindab Group's fundamental approach to cyber security and compliance. They provide a consistent foundation for the development, implementation, and operation of security controls and practices across the organisation.

Shared responsibility

Everyone, employees, managers, and partners, shares responsibility for protecting Lindab Group's information, systems, and operations as part of their daily work.

Governance, accountability and risk ownership

Lindab Group establishes and maintains clear roles, responsibilities, and decision authority for information security, cyber security, and compliance related matters.
Cyber and information security risks have a named owner and are actively managed, followed up, and escalated when needed.

Risk-based and proportionate security

Information and cyber security risks are identified, assessed, and managed based on business impact and likelihood. Security controls are selected and prioritised to reduce the most significant risks first, ensuring protection is effective and proportionate with a defined risk appetite indicating the level of risk exposure acceptable for the organisation. Access to information and systems shall be governed by the principles of least privilege and Zero Trust, ensuring that no implicit trust is granted based on network location, asset ownership, or user identity alone.

Baseline and Enhanced Security Requirements

Minimum security requirements, as stated in related security directives, must be applied as a security baseline across the organisation. Areas with higher risk, criticality, or regulatory exposure are subject to enhanced security controls proportionate to the level of risk. Lindab Group recognises the distinct security challenges of Operational Technology (OT) and SCADA systems and commits to applying tailored controls and risk management practices to protect these environments.

Asset Management and Ownership

All information assets are identified, classified, documented and assigned an owner. Owners are responsible for ensuring appropriate protection throughout the full lifecycle from creation and use to storage, change, and disposal.

Secure by Design and by Default

Security and privacy are built into the design, procurement, development, implementation, and operation of systems, services, and business processes. Security is not added afterwards; it is part of how Lindab designs and operates.

Legal, Regulatory, and Contractual Compliance

Information and cyber security practices must comply with applicable legal, regulatory, and contractual requirements. Compliance is a minimum expectation and a foundation for trust.

People, awareness, and responsibility

Employees and relevant third parties must understand and follow information and cyber security requirements appropriate to their roles and responsibilities. Awareness, training, and responsible behaviour are essential to reducing risk. In addition, cyber security, risk, and compliance responsibilities should be clearly incorporated into competence profiles to ensure these expectations are recognised and embedded within the organisation.

Third-Party and Supply Chain Security

Cyber security risks related to suppliers, partners, and other third parties are identified and managed throughout the entire relationship lifecycle, including contracting, operation, and exit.

Incident Management and Resilience

Security incidents must be identified, reported, managed, and learned from in a timely and structured manner to minimise impact and ensure resilience. Lindab Group fulfils applicable regulatory reporting obligations, including but not limited to the incident notification requirements under the NIS2 Directive, as defined by relevant legal and regulatory requirements.

Continuous Improvement

Cyber security is managed proactively and continuously reviewed and improved to address evolving threats, risks, and business changes.

Scalability and Adaptability

Security controls and processes are designed to scale and adapt as Lindab Group’s business operations, technology, and the threat landscape evolve.

6. Cyber Security and Compliance Framework

Lindab Group's Cyber Security and Compliance Framework (hereinafter referred to as Framework) is based on the ISF Standard of Good Practice (SoGP) and is aligned with relevant international standards and frameworks, including ISO/IEC 27001 and NIST Cybersecurity Framework (CSF). The framework is aligned with regulatory requirements including the NIS2 Directive and the Cyber Resilience Act (CRA) where applicable.

The Framework is structured into cyber security capabilities. A cyber security capability is Lindab Group's ability to consistently perform a set of activities that manage cyber risk and protect information, systems, and services over time. In practice, a capability is not "a tool" and not "a control checklist". It is an operating ability that combines:

- People: defined roles, skills, responsibilities, ownership.
- Process: repeatable ways of working, procedures, decision points, escalation paths.
- Technology: tools and technical controls that enable and scale the process.

Lindab Group Framework is structured into the following capabilities, each defining requirements for secure operations within the organisation and across our external relationships (e.g. suppliers, service providers, and partners):

- Security Governance & Strategy
- Risk, Threat & Intelligence Management
- Asset and Information Management
- Identity and Access Management
- Vulnerability & Exposure Management
- Security Architecture & Secure Engineering
- Third-Party and Supply Chain Security
- Security Operations & Incident Response
- Resilience, Crisis & Continuity Management
- People, Awareness & Security Culture
- Security Assurance & Control Validation
- Privacy, Compliance and Legal Risk
- Physical & Environmental Security

6. 1 Framework structure

The framework is aligned with Lindab Group Policy Framework

Policy – Define principles, governance structure, strategic intent and accountability.

Directive – Define mandatory security requirements and controls per area.

Guidelines – Define how requirements are fulfilled in practice

Procedures – Define details on how requirements are fulfilled in practice.

7. Governance model

Lindab Group applies a Three Lines of Defence model to ensure that cyber security risks are effectively managed, monitored, and independently validated across the organisation.

First Line – Operational Ownership

Business and IT functions are responsible for managing cyber security risks within their day-to-day operations. This includes implementing and maintaining required security controls and ensuring they operate effectively.

Second Line – Oversight and Governance

The Cyber Security and Compliance function is responsible for defining requirements, providing guidance, monitoring risk, and ensuring alignment with business objectives and applicable obligations.

Third Line – Independent Assurance

Independent assurance validates the effectiveness of the Framework and its controls. Findings and recommendations are reported to the Board and Group Management Team to support oversight and continuous improvement.

The Board retains ultimate accountability for cyber security and compliance across the organisation. The CISO shall report periodically, and no less than once every 6 months, to the Board or its designated committee on the status of cyber security risk, compliance posture, and material incidents. Significant risks or incidents shall be escalated to the Board without undue delay.

8. Roles and responsibilities

The following roles and responsibilities establish accountability and ensure effective execution, monitoring, and continual improvement of the Framework. Regional or Local definitions might exist for equivalent roles.

Role	Responsibility
Board of Directors	• Provides strategic oversight and ultimate accountability for information and cyber security. • Approves the Cyber Security and Compliance Policy and related strategies. • Reviews periodic reports on cyber risk and assurance activities.
Group Management Team	• Ensures that adequate resources are allocated to manage cyber security risks. • Integrates cyber security objectives into business planning and decision-making. • Supports enforcement of policy and ensures alignment with organisational strategy. • Ensure governance, priorities and resources for Crisis management and Business Continuity Management.
CIO	• Policy Owner for the Cyber Security and Compliance policy.

	• Ensures adequate IT governance structures are in place to support the implementation of the Cyber Security and Compliance Framework.
	• Ensures that IT investments and projects incorporate security requirements from inception.
CISO	• Owns, maintains and continuously improves the Framework.
	• Defines this policy, supporting directives, and guidelines.
	• Monitors compliance, reports on risk exposure, and coordinates security governance across the organisation.
	• Owns, maintains and continuously improves Incident Management capabilities (SOC, incident investigations, forensics).
	• Owns, maintains and continuously improves Service management operations, awareness and training, compliance (service offering) and related capabilities including processes, and tools (Service catalogue).
DPO (Data Protection Officer)	• Ensures that the organisation's processing of personal data complies with applicable data protection legislation.
	• Advises and informs the organisation and its employees of their obligations under data protection law.
	• Monitors compliance with data protection policies, directives, and guidelines.
	• Acts as the primary point of contact for data protection authorities and data subjects regarding matters related to personal data processing.
	• Conducts and supports Data Protection Impact Assessments (DPIAs) for processing activities that may result in high risk to individuals.
	• Maintains records of processing activities and ensures that data protection considerations are integrated into relevant processes and systems.
	• Escalates data protection risks and incidents to the Group Management Team and relevant authorities as required by law.
Information Owner	• Responsible for initiating and approving information classification, identifying security requirements, and ensuring appropriate protection of the information throughout its lifecycle. The role represents the business interests of the information and collaborates with IT, security, and process owners.
	• Has mandate to decide whether information processing may be initiated, continued, or significantly changed.

System Owner	• Ensure appropriate security controls are implemented for assigned assets. • Review risks and access rights related to their system. • Decide on the commissioning, deployment, and major changes to systems. • Define the scope of systems and services for which they are responsible. • Ensure that systems support the security requirements defined by relevant information owners.
Service Owner	• Responsible for the lifecycle management of an assigned service, ensuring that security requirements are defined, implemented, and maintained throughout the service lifecycle. • Acts as the primary point of accountability for security compliance, risk management, and continuous improvement within the scope of their service, and collaborates with capability owners, system owners, and third parties as required.
Capability owner	• Responsible for ensuring that the organisation can effectively manage and operate its capability, maintaining compliance with relevant directives and continuously improving the capability over time. • Ensure that risks are identified, mitigated, and escalated according to policy. • Participate in audits, reviews, and incident management activities.
Regional IT Manager	• Responsible for ensuring that information and cyber security requirements are implemented and maintained across assigned regional IT operations, acting as the primary point of accountability for security compliance, risk escalation, and alignment with Lindab's Cyber Security and Compliance Framework within the region.
Local IT Manager	• Responsible for the day-to-day implementation and maintenance of security controls within the local IT environment, ensuring compliance with Lindab's security requirements, and escalating risks and incidents to the IT Regional Manager or relevant capability owner in a timely manner.
Employees and consultants	• Comply with Cyber security and Compliance policy, directives, and guidelines. • Protect information and report security incidents, weaknesses, or policy violations promptly. • Complete mandatory awareness and training activities.

Third Parties	• Comply with contractual information security requirements. • Protect Lindab's information in accordance with agreed controls. • Report information security incidents affecting Lindab's information.

9. Supporting directives

The following topic-specific directives support this policy:

- Acceptable Use Directive
- Security Governance & Strategy Directive
- Risk, Threat & Intelligence Management Directive
- Security Architecture & Secure Engineering Directive
- Asset Management Directive
- Identity & Access Management Directive
- Vulnerability & Exposure Management Directive
- Security Operations & Incident Response Directive
- Third-Party & Supply Chain Security Directive
- Resilience, Crisis & Continuity Management Directive
- Security Assurance & Control Validation Directive
- Privacy, Compliance & Legal Risk Directive
- People, Awareness & Security Culture Directive
- Physical & Environmental Security Directive
- Data Protection Directive
- Generative AI Directive

See appendix for complete list of supporting appendices intended to be used together with each directive.

10. Review

This Policy shall be reviewed as set out in Lindab Group Policy Framework, or following significant organisational, technological, or regulatory change. CISO is responsible for ensuring the framework remains current, effective, and aligned with Lindab Group’s strategic objectives.

11. Document control and version management

This policy shall be subject to formal version control according to Lindab Group Policy Framework.

Lindab Group

Appendix A – Glossary of Terms and Abbreviations

A.1 Definitions

Term	Definition
Asset	Any information, system, service, or resource that has value to the organisation and requires protection. a) a primary asset is an asset in the form of processed information or a provided service, b) a supporting asset is an asset ensuring the functioning of primary assets, in particular an employee, supplier, technical asset, building and other limited space in which the regulated service asset is located, and c) a technical asset is a technical or software device or equipment.
Capability	The organisation's ability to consistently perform a set of activities that manage cyber risk and protect information, systems, and services over time. A capability combines people, process, and technology.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Cyber Security	The practice of protecting systems, networks, applications, and data from digital attacks, unauthorised access, damage, or disruption.
Directive	A topic-specific document that defines mandatory security requirements within a defined area, subordinate to this policy.
Governance	The system of rules, practices, and processes by which an organisation directs and controls its security activities and accountability structures.
Information Asset	Any information held or processed by the organisation, regardless of format, digital, physical, or verbal, that has value and requires protection.

Information Security	The protection of information assets against unauthorised access, use, disclosure, disruption, modification, or destruction, to ensure confidentiality, integrity, and availability.
Integrity	The property of safeguarding the accuracy and completeness of information and processing methods.
Availability	The property of being accessible and usable upon demand by an authorised entity.
Operational Technology, OT	Hardware and software used to monitor and control physical processes, devices and infrastructure, such as industrial control systems, SCADA and PLCs.
Policy	A high-level governance document that establishes principles, requirements, and accountability structures, approved by senior management.
Risk	The potential for an event or action to negatively affect the organisation's ability to achieve its objectives, expressed in terms of likelihood and impact.
Risk Appetite	The amount and type of risk that the organisation is willing to accept in pursuit of its objectives.
Risk Owner	An individual with the accountability and authority to manage a specific risk.
Resilience	The organisation's ability to anticipate, withstand, recover from, and adapt to adverse events, including cyber incidents, disruptions, and crises, while maintaining continuity of critical operations and services.
Security Control	A safeguard or countermeasure designed to protect the confidentiality, integrity, and availability of information and systems.
Security Incident	An incident that has, or could have, an adverse effect on the security or operations of the organisation, including breaches, intrusions, and policy violations.

Supply Chain	The network of suppliers, vendors, partners, and service providers involved in delivering products or services to the organisation.
Third Party	Any external organisation or individual, including suppliers, partners, consultants, and contractors, that accesses, processes, or manages Company's information or systems.
Threat	Any circumstance or event with the potential to cause harm to information assets, systems, or operations.
Vulnerability	A weakness in a system, process, or control that could be exploited by a threat to cause harm.

A.2 Abbreviations

Abbreviation	Full Term
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Organization for Standardization
NIS2	Network and Information Security Directive 2
RACI	Responsible, Accountable, Consulted, Informed
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Centre
SoGP	Standard of Good Practice (ISF)