knowit

Information Security and Data Protection Policy

SUMMARY

This policy establishes the framework for the direction, organization, and accountability for our collective information security and data protection initiatives, and is to be adhered to by all entities, employees, and contractors within the Knowit Group.

Purpose and goal

The purpose of this policy is to specify the direction, organization and the accountability for our joint information security and data protection efforts. This policy, related guidelines and instructions shall be followed by all companies, employees, and contractors within the Knowit Group.

Knowit are committed to ensure continual improvement and effectiveness of the Information Security as an integral part of our overall Business Management System (BMS). Knowit shall continuously ensure the protection of our customers and our own assets against both intentional and unintentional threats to be compliant with applicable legal, regulatory, and contractual requirements, as well as other business requirements and expectations. Applicable regulatory requirements include, but are not limited to, the General Data Protection Regulation (GDPR), the NIS2 Directive, the EU AI Act, and sector-specific obligations arising from Knowit's role as a provider of digital and trusted services. Knowit further adheres to industry assurance schemes, including TISAX.

Knowit´s overall goals for information security and data protection are:

- **Confidentiality** – Information shall only be accessible to authorized persons.
- **Integrity** – Information, and the results of information processing, shall be correct.
- **Availability** – Information and information systems shall be available when needed.
- **Traceability** – Accessing, changing, or creation of information shall be registered and traceable to individual users.
- **Privacy** – Information shall be collected, shared, and used only in ways that respect and safeguard the rights of individuals.

Risk-based security

Knowit aims to minimise security risks in the most cost-efficient manner. The cost of a security measure must be analysed in relation to the anticipated reduction in risk resulting from the implementation of that security measure. This assessment is done during the risk analysis.

Risk analysis is a vital part of Knowit´s information security and data protection process and shall be integrated in our business and support processes including all major changes within our

operations and business. Risk assessments shall address third-party and supply chain dependencies, the use of AI systems and AI-generated outputs, and threat intelligence.

Implementation

To support our work with information security and data protection, Knowit utilises a Business Management System, based on the international standard ISO/IEC 27001.

Guidelines, instructions and procedures supporting this policy shall be made easily available to relevant stakeholders.

All companies and individuals that have access to Knowit´s or Knowit´s clients´ premises, assets or information shall read this policy. Temporary visitors to Knowit´s facilities are not bound by this requirement.

Relevant stakeholders shall be informed about significant changes to this policy. Knowit shall also continuously work to improve stakeholder understanding and implementation of current information security and data protection requirements.

Responsibilities

All stakeholders within Knowit share the responsibility for information security and data protection.

- The **Chief Security Officer (CSO)** serves as leader and coordinator for information security within the Group. The CSO is responsible for maintaining the ISMS and supports the organization in matters related to information security.
- The **Data Protection Manager (DPM)** serves as leader and coordinator for data protection within the Group. The DPM is overall responsible for the compliance with the General Data Protection Regulation (GDPR) (and other applicable data privacy legal acts) and supports the Group in matters related to data privacy.
- All **managers** are directly accountable for compliance with this policy within their area of responsibility.

Information Owners shall be identified for all business-critical information assets, including processes, systems, and information. The Information Owner shall ensure that information is classified and assigned the appropriate level of protection.

Knowit shall maintain the capability to notify competent authorities of significant incidents within 24 hours (early warning) and submit a full incident report within 72 hours.

Monitoring and reviewing

The effectiveness of this policy shall be measured continually. The policy shall be reviewed at least annually. Additional reviews shall occur when Knowit makes operations or business changes that might significantly affect this policy. These reviews are the responsibility of the CSO.

Stockholm 2026-08-31

Fredrik Walde Ekerhovd, CEO Knowit Group