avonova

INFORMATION SECURITY POLICY

GROUP STEERING DOCUMENT

Version	Approved by BoD	Document owner
Ver. 1.0	DD.MM.202Y	CISO

Content

Purpose

Avonova's Information security policy is designed to support Avonova's business initiatives and strategy to achieve our goal and vision. The policy and the supplementary Information security procedures govern how Avonova and its subsidiaries manage, operate and control their information security on a strategic, tactical and operational level, to enforce a risk-based and systematic approach to information security. It aims to guide and support Avonova in protecting company assets from both internal and external threats.

Scope and responsibilities

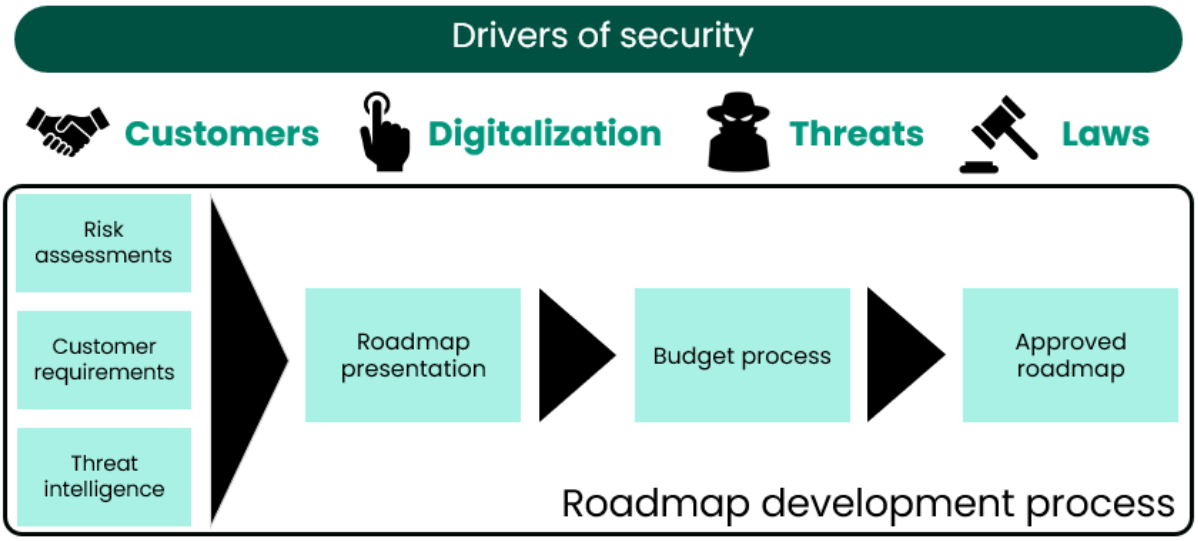
This group policy applies to all company assets, all Avonova legal entities, locations, employees, consultants, and others that have access to any of Avonova's IT resources, including all information, IT systems networks, equipment, and facilities.

Role	Responsibility
Board of directors	Policy approval.
Management	Management is responsible for ensuring that an approved, updated and communicated information security policy is established.
CISO	Avonova's CISO is responsible for maintaining the policy, verifying the necessary systems, tools and support are available, confirming the effectiveness and compliance of the policy and measuring and reporting results to management.
Employees & contracted personnel	All employees and contracted personnel are responsible for understanding and following this policy and its supplementary procedures where it applies to their duties and workflows.

Policy

Strategic direction

Avonova's information security strategy is built around Avonova's business strategy and the four key driving areas of security. It is implemented through Avonova's information security management system based on the ISO 27001:2022 standard and is comprised of a governing policy, supplementary Information security procedures and individual processes, controls and routines. Security initiatives are selected and prioritized based on risk and cost-effectiveness and are implemented through a security roadmap. The roadmap is annually developed in agreement with Avonova's business plan and with an approved budget from Avonova's IT budget.



Security objectives

Security objectives are set for each security domain in the supplementary security procedures, the security roadmap implementation progress, and for Avonova's security hygiene controls.

Information security procedures

Each security domain has its own security objectives defined in the Information security procedures document.

Roadmap

Avonova's security roadmap shall be carried out according to plan. Changes to the security roadmap shall be reported to management.

Security hygiene

Avonova tracks several metrics to build a summarized risk level and security status based on (Vulnerabilities, incidents, Security awareness, security alerts, patch management). Measured and reported quarterly to management.

Principles

These principles set the standards that Avonova's information security work should conform to when designing and implementing information security in the company.

- **Ethical**
  Avonova's information security must be compliant with governing laws of areas where Avonova is operative.

  Sweden

  - Patientdatalagen
  - Dataskyddsförordningen (GDPR).
  - Patientsäkerhetslagen
  - Cybersäkerhetslagen (NIS2)

- Arbetsmiljölagen

Norway

- Arbeidsmiljøloven med tilhørende forskrifter
- Lov om behandling av personopplysninger
- NIS2
- Helseregisterloven
- Helsepersonelloven
- Personopplysningloven (GDPR)
- Pasientjournalloven
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)
- Forskrift om utførelse av arbeid og Forskrift om pasientjournal

Finland

- Tietosuojalaki, 1050/2018 (GDPR)

- **Uniform**
  The information security work at Avonova shall be structured and encompassing. Assets shall be managed through proven processes in accordance with industry standards and best practices. Processes shall be executed consistently and systematically throughout the organization.

- **Inclusive**
  The information security work at Avonova shall be inclusive. Avonova shall foster a prevalent security culture within the organization, where individuals and the organization share a common understanding of values, risk behavior, and attitude. Both individuals and the organization shall work together toward established goals.

- **Versatile**
  The information security work at Avonova shall be adaptable. The efforts undertaken shall align with the company's business objectives, strategies, and vision. The work shall not hinder the organization's development but rather enable it in a secure manner.

- **Quality**
  The information security work at Avonova shall be characterized by quality and strive for continuous improvement. Avonova shall measure and evaluate the effectiveness of its work annually against set goals. These goals shall be established and revised in accordance with Avonova’s needs.

- **Integrated**
  The information security work at Avonova shall be integrated. Information security shall be an integral part of the business and be considered in all processes and departments within the organization.

- **Sustainable**
  The information security work at Avonova shall be sustainable and cost-effective, with long-term goals in mind. Information security efforts shall be conducted at strategic, tactical, and

operational levels, where the tactical and operational parts are anchored to a strategic vision.

Governance

This policy and supplementary Information security procedures are governed by IT to ensure Avonova's ability to stay compliant with regulations and protect the organization's assets against threats and damages. They are reviewed annually, and effectiveness is measured through follow-up controls and internal audit. Any change or exception to the policy needs to be documented and approved by management.

Deviations from policy

Any breach of this policy shall be reported to Avonova's CISO, be risk evaluated and documented in Avonova's risk management system (Risma).

References