Information Security Policy

This policy is a statement of intent and the overall guideline for decision-making and achieving desired goals. The Information Security Policy is the overarching document in Coromatic's Information Security Management System (ISMS) and belongs to the Coromatic security process.

The goal of this policy is to protect and ensure information within our daily business; we shall protect our customers, Coromatic as a company and a brand and our employees and partners. Our protection shall be adapted to protect values, risks and legal requirements and thereby achieve our goals.

Security is quality - quality is safety

The policy governs information security and covers all employees, sub-contractors and parties acting in the name of Coromatic. The Information security policy is accompanied by guidelines, instructions and methods for how Coromatic oversee and manage information security tasks. Coromatic complies with ISO / IEC 27001 regarding requirements, documents and standards for the management, improvement and audit of the ISMS.

Information and information assets refers to all information, whether processed manually or automatically, and regardless of the form or context in which it is produced or transferred. Information security is defined by its confidentiality, availability, integrity and accountability.

Information security is defined by:

- ***Confidentiality*** refers to ensuring that information is accessible only to those employees who are authorized to access it.
- ***Availability*** refers to ensuring that authorized users, if necessary, have access to the information and associated assets they need.
- ***Integrity*** refers to the protection of information to hinder altering or deleting it.
- ***Accountability*** refers to that actions of an entity may be traced uniquely to that entity

The intent of this policy is to protect Coromatic information assets from threats - internal or external, accidental or deliberate. Information security is a natural part of Coromatic's' everyday business and our business processes.

Management commitment

Information security must be an integral part of operations in Coromatic. All process owners, executives, and owners must promote continuous improvement and establishment of safety and security culture within Coromatic.

The management system for Coromatic also consists of the following documents:

- Guideline
- Instructions
- Templates and checklists

Responsibilities

All employees are responsible for following, developing and constantly improving the management system.

Process owners are responsible for ensuring that all employees are informed and educated about the policy.

Information owners are responsible for processing information in cases where the CEO is not the overall owner of the information.

Ultimately, the responsibility for management of information security within Coromatic is the CEO. Operational responsibility for the management, compliance of security processes and continuous improvement is the CSO.

Anyone who uses information assets in a manner that violates this policy may be subject to disciplinary action or criminal sanctions.

Stockholm, 14th of February 2018

Coromatic Group AB

Erik Bertman

CEO