Group Information Security Policy

1. Introduction

The purpose of information security is to ensure the confidentiality, integrity, and availability of information resources. This Information Security Policy is a management approved statement of the objectives, roles, responsibilities, and implementation of Evac Group's (hereinafter Evac) information security. This policy is reviewed on a yearly basis, as well as when significant changes occur.

Throughout this policy and related Practice documents, the term "user" identifies full-time and part-time employees, contractors, consultants, service providers, temporaries, student assistants, volunteers, vendors, customers, and other affiliated parties who access Evac technology resources.

2. Scope

This policy applies to all users in all countries using information and communication technology provided by Evac and its service providers. This policy is complemented by relevant Group Practice documents, which provide more detailed information, rules and requirements concerning information security.

This policy is not intended to ensure compliance with personal data protection regulations. While personal data protection is covered under other Evac policies, information security does provide methods of fulfilling security-related personal data protection requirements.

3. Objectives

Evac creates, stores, and utilizes information with significant financial value, such as product, project, and financial data, as well as other trade secrets and intellectual property. This information is sensitive, and Evac must ensure that it is kept confidential.

Evac has legal and contractual responsibilities to protect specific types of information, such as personal data and customer data. Certain projects and customer relationships, such as those related to naval vessels, subject Evac's operations to strict security requirements. Evac must ensure compliance with all information security obligations from both contracts and legislation.

Evac's business processes rely on numerous information systems from workstations and email to ERP and PLM applications. The availability of these systems must be ensured.

Evac uses data and information systems for decision-making and executing significant actions, such as financial transfers. The integrity of such data must be protected and access to significant actions within information systems must be controlled.

Evac delivers a wide variety of products with automation and as these become increasingly digital and connected, the importance of their security increases. In the space of digital services and connected products, it is essential that customers can trust the security of Evac's products and services.

4. Roles and responsibilities

Everyone at Evac is responsible for information security on their own behalf. All users are required to follow the given policies and instructions as well as to report all identified information security risks and potential incidents without delay.

All employees working in management roles are responsible for supervising the activities and level of information security awareness amongst their team members and must intervene when identifying actions that conflict with this policy.

This policy is owned by the Group Head of ICT, who is responsible for defining, implementing, and updating this policy, as well as for monitoring and reporting on its execution. The Chief Financial Officer makes decisions on Evac's response to suspected policy violations.

The Evac Group CFO approves this Group Policy and updates to it.

ROLE	RESPONSIBILITY
Group CFO	Approves Group Information Security Policy Decides response to suspected policy violations
Head of ICT	Owns information security management

5. Reporting and continuous improvement

Information security management at Evac is performed in a risk-based manner. Using a risk-based approach, resources and investments are allocated to high value and high priority development areas and issues. The Head of ICT is responsible for monitoring changes to Evac's information security risks and adjusting activities accordingly to ensure continuous improvement of Evac's information security management system.

The Head of ICT is responsible for monitoring the execution of this policy and reporting on it and any other relevant information security matters to the Group Leadership Team and Board of Directors at minimum on a quarterly basis.

6. Laws and regulations

Evac operates in several different jurisdictions. Should local legislation or regulation, or the specific situation of any unit in Evac require more stringent rules than what is defined in Evac's policies, the relevant unit must adhere to them and, consequently, respective governing documents shall reflect those requirements. Evac follows the legislation and regulations of each specific country on information security and protection of personal data.

7. Violations

All actions against the approved Information Security Policy and related Group Practices are regarded as violations. These violations may lead to disciplinary actions based on the severity of the violation, up to and including termination of employment and possible civil and/or criminal prosecution to the full extent of the law.

8. Related documents

The implementation of this Policy is further described in Evac's information security related Group Practice documents, as well as in other Evac policies. A list of current policies and practices is available on Evac's intranet.

9. Approval

This Group Information Security Policy version 1.2 has been approved by Evac Group CFO.

Change log

Date & version	Changes	Editor
8.8.2022 v1.0	First release	Kristian Herland
9.3.2023 v1.1	Changed responsibilities from ISO -> Head of ICT	Sami Niemelä
31.10.2023 v1.2	Review: minor visual edits, no changes to content.	Sami Niemelä