Information Security and IT Policy

The core mission of Suomen Malmijalostus results in the accumulation of information related to the construction of the mining industry and battery value chain, including business secrets. Significant amounts of protected information related to financing and contracts are also accumulated.

Suomen Malmijalostus's mission requires the development of cooperation networks with domestic and foreign companies and other organizations. The goal is to create new business and innovation in Finland.

Therefore, it is important to safeguard the business secrets and other confidential information held by the company from misuse. The continuity of operations of Suomen Malmijalostus and its subsidiaries must also be ensured.

The Security and IT Policy guides the development of security and IT operations. The goal is to protect operations from security threats, ensure continuity, and enable efficient operation of the organization with customers, owners, employees, partners, and other stakeholders.

Responsibility is emphasized in the company's core mission. The ISO 26000 standard is utilized as a handbook for responsibility. The goal of the Security and IT Policy is to enable the realization of responsibility in operations.

The company's security and IT operations are mandated and guided by national and international general legislative obligations as well as industry-specific special legislative obligations.

We comply with current and relevant regulations for security, including the following:

- Data Protection Act and EU General Data Protection Regulation (GDPR)
- Accounting Act and Accounting Regulation
- Trade Secrets Act and Act on the Protection of Privacy in Working Life
- Authority permits
- Other regulations relevant to security (e.g., NIS2 Directive)

Application

The Security and IT Policy is applied in all operations of Suomen Malmijalostus and its wholly-owned subsidiaries. All employees of Suomen Malmijalostus and its wholly-owned subsidiaries comply with the policy.

Partners and subcontractors comply with the policy to the extent required by Suomen Malmijalostus as the client.

Principles

We identify critical information, systems, and tools for the operations of Suomen Malmijalostus. Special attention is paid to their development, and their security risks are handled according to a pre-agreed process.

To support secure working, we publish and comply with security principles and guidelines that describe security methods concretely.

To ensure continuity of operations, security and IT operations are developed in the following ways:

- Company information is classified and protected accordingly
- Procedures for assessing and managing security and IT operation risks are followed in all operations
- Security awareness and the efficient and secure use of information systems and tools are improved and maintained through training, guidance, and communication to staff
- Security incidents are reported, handled, and monitored
- Continuity management and development of critical information systems, tools, and services are invested in by classifying critical systems, tools, and services and monitoring their risk levels and development
- Transition from local server-based applications to cloud services

Management and Organization

The strategic management of Suomen Malmijalostus's security and IT operations is the responsibility of the management team and the group's CFO.

The operational guidance and development of security and IT operations are the responsibility of the IT development and security working group, which has diverse representation from different functions.

Responsibilities for different roles are set as follows:

Board of Directors

- Approves the Security and IT Policy
- Monitors compliance with the policy

Management team and especially the CFO

- Responsible for the strategic management of security and IT operations

- Regularly reviews the principles of security and IT operations
- Reports serious security deficiencies and deviations from the policy to the Board of Director
- Decides on security-critical systems

Security and IT development working group

- Guides the development and implementation of security and IT operations and carries out necessary minor development
- Meets regularly
- Leads the assessment of security and IT operation risks and the handling of significant risks
- Prepares development proposals for the management team as needed
- Makes development decisions when they do not require management team handling
- Responsible for maintaining the principles of security and IT operations

Approval and Interpretation

The Board of Directors of Suomen Malmijalostus Oy has approved this Security and IT Policy on March 17, 2025. The CEO of Suomen Malmijalostus Oy is responsible for the implementation of the policy. The CFO, a member of the management team, is responsible for monitoring the application and interpretation of the policy