

Information Security Policy

1. Purpose

MAGNETEC's security policy defines the guidelines and measures necessary to protect the confidentiality, integrity, and availability of information within our company. Compliance with this policy is required to ensure the security of our data, systems, and services and to meet legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, consultants, and other third parties who have access to the company's systems and information. It covers all data and information systems of the company, regardless of whether they are located in our offices, data centers, or on mobile devices.

3. Responsibilities

- **Management:** Management is responsible for providing the necessary resources to implement this policy and holds overall responsibility for information security within the company.
- **IT Security Officer:** The IT Security Officer is responsible for the development, implementation, and monitoring of security measures, as well as for training employees.
- **Employees:** All employees are required to comply with this policy and participate in information security training. They must ensure that they do not disclose information without authorization or transfer it to insecure environments.

4. Principles

- **Confidentiality:** Information may only be accessed or processed by authorized persons. All employees are required to treat sensitive data confidentially and use it only for legitimate business purposes.
- **Integrity:** The accuracy and completeness of information must be ensured at all times. Employees are required to maintain the information in the systems correctly and to make changes only according to established procedures.
- **Availability:** Information must always be accessible and usable by authorized users. Appropriate measures must be taken to protect systems against failures and data loss.

5. Access Control

Access to the company's information systems and data must be strictly controlled. Users must be clearly identified and authenticated. Permissions are granted based on the principle of least privilege, meaning that users are given only the permissions they need to perform their tasks.

6. Security Measures

- **Technical Measures:** These include firewalls, antivirus software, encryption technologies, and regular security updates for all systems.
- **Organizational Measures:** These include the definition of responsibilities, conducting risk assessments, emergency plans, and regular security audits.
- **Physical Measures:** These include controlling access to office spaces, server rooms, and other sensitive areas through locks, access cards, and surveillance cameras.

7. Training and Awareness

All employees must regularly complete information security training to ensure they are informed about current threats and best practices in handling information. Awareness programs are designed to promote a culture of security throughout the company.

8. Incident Management


Security incidents must be reported immediately and handled according to the established emergency plan. All employees are required to report any suspicious activity or security breaches to the IT Security Officer immediately.



signed by
Marc Nicolaudius
MANAGING DIRECTOR



signed by
Andreas Becker
HEAD OF QUALITY



signed by
Gabor Zsak
IMS LEADER