Meijers
insurance
brokers

Meijers Information Security

At Meijers we find availability, integrity and confidentiality of information (services) important. That is why we take information security measures that match the risk profile of the organisation. For example, we comply with the requirements for information security and privacy legislation (General Data Protection Regulation). Our information security policy is based on the most recent version of the internationally recognized ISO27001 standard.

Why is information security important?

With the information security measures we take, we ensure the desired level of availability, integrity and confidentiality of Meijers' information facilities.

- Availability: The business continuity, recoverability and redundancy of information (systems).
- Integrity: The correctness, completeness and timeliness of information and the correct functioning of ICT resources.
- Confidentiality: The protection of information against unauthorized access, related to privacy protection and the exclusivity of information.

Information security relates to all forms of information within Meijers and is therefore an essential part of business operations. Information security therefore falls under the direct responsibility of the executive team and management. Information security applies to all employees, processes, information flows, information systems, information carriers and third parties that are deployed on behalf of Meijers.

Information Security Management System

In order to achieve a sufficient level of information security in line with the risk attitude, Meijers uses an Information Security Management System in accordance with the 'Plan, Do, Check, Act' cycle.

Plan:

- Drafting of an information security policy and defining priorities
- Setting up processes and procedures and making capacity (people and resources) available

Do:

Information security is a structural and active part of business operations. This is proactively implemented by, among other things:

- Performing system classifications and risk assessments
- Setting up authorization matrices
- Prescribing additional security measures
- Providing awareness training to employees

Check:

To obtain guarantees regarding the operation of the policy, compliance with the policy is measured periodically by:

- Review of periodic reports
- Assessment of external services
- Performing clean desk and clear screen checks
- Conducting penetration testing on critical environments

Act:

Meijers acts when reported deviations or new (external) threats so require. In addition, the findings of internal and external audits and assessments are followed up.

Information Security Measures

Because availability, integrity and confidentiality of information (services) are important to Meijers, we take below measures when it comes to information security.

Asset Management

We register company resources [assets] which give access to company-sensitive information. We also appoint a user and arrange for maintenance and implementation of associated security measures.

Staff and hiring

We screen new staff and third parties. They also sign a nondisclosure agreement. We ensure that information security responsibilities are laid down contractually.

Physical Security

Only authorized persons have access to the Meijers digital environments. Guests are always accompanied by a Meijers employee. Company sensitive information is not left unattended. A 'clean desk' and 'clear screen' procedure applies to all workplaces.

Operational ICT management

In order to guarantee reliable information processing, we have established operational responsibilities and procedures regarding ICT. Important measures are policy on updates and backups, protection against malware, handling of mobile data carriers and network security.

Access security

Certain measures ensure that the authentication and authorization of users and administrators takes place in a correct and comprehensive manner. The authentication and password policy include minimum password complexity, length and change frequency. Where necessary, we will make use of an additional two-factor authentication.

Incident management and data breaches

We record and follow up on security incidents to limit business damage and prevent recurrence.
Suppliers are part of this procedure.

Business Continuity Management & Disaster Recovery

We have a Business Continuity Plan & Disaster Recovery plan for dealing with major calamities that can seriously disrupt business operations. This plan is updated and tested periodically to ensure proper functioning.

Information Security and Suppliers

We expect suppliers' security measures, insofar as this affects Meijers information and/or information security, to be at least at the same level as Meijers. We check that suppliers who are important to our information security are compliant with this.

Every year we request ISO27001 or comparable certifications from our main suppliers. In addition, we have the right to perform additional audits (right to audit). If suppliers use subcontractors, we establish that they meet the same standards as the supplier.

meijers

a sure step forward

Van Heuven Goedhartlaan 935
1181 LD Amstelveen
Postbus 707
1180 AS Amstelveen

+31 (0) 20 642 05 24

info@meijers.nl
www.meijers.nl