Policy statement

An information security management system is created with the aim of achieving set policy objectives. ARS T&TT management has defined the company's information security policy in this statement.

The management is responsible for both the policy and the maintenance of the management system. It follows that management undertakes to provide sufficient people and resources to maintain the IB system and to ensure that the management system is planned to meet the goals and meet the requirements. The formulated policy provides a framework for drawing up and periodically assessing information security objectives.

ARS T&TT's policy has the following objectives:

- promoting an efficient work culture
- continuously improving its services and products
- increasing customer satisfaction
- protecting the confidentiality, integrity and availability of confidential information
- positively influencing and raising the awareness of its staff about their role in the areas addressed by management systems
- give stakeholders the confidence that risks are controlled.

The management wants to achieve these goals by:

- work in accordance with the requirements of NEN-ISO/IEC 27001
- legal requirements and other requirements that the company endorses
- achieving efficiency benefits
- continuous improvement of the ISMS
- avoiding risks in the field of information security
- preventing complaints and incidents
- making the necessary resources available to achieve the goals and to increase effectiveness
- promoting awareness of employees in the field of information security
- providing clarity in the responsibilities, powers and mutual relationships of all employees
- increasing the competitiveness of the organization
- providing tools to train (new) employees
- recording the existing craftsmanship in the organization
- recording customer satisfaction statements
- being aware of the latest state of the art techniques and implement these if possible
- using experiences gained inside and outside the company.

It is important that all employees understand the policy, put it into practice and keep it up to date at all levels in the organization. For this reason, the Security Officer informs employees about the content of this policy statement.

The management of the organization ensures that changes within the information security system do not affect the integrity of the system by conducting a risk assessment in advance and adopting control measures for identified risks.

All risks and threats are reported internally, and where necessary externally, and used to continuously improve the working methods in place.

The organization will, in the performance of its task, respect all stakeholders, while respecting the principles of data security.

Ensuring information security is a priority for the company.
In addition to the standard standards and values, additional measures have been taken in the context of information security to increase (information) security and to guarantee it as much as possible.
The ISMS of the organization is focused on the activities as stated in the scope. The ISMS policy is aimed at controlling (risks of) information security. The necessary procedures have been drawn up for this with regard to company resources, employees, physical security, communication, access policy, information systems, business continuity and legal requirements.

The management system applies to all (temporary and hired) employees.

A risk analysis was performed for the ISMS business processes based on CIA with a structure using the Worth Kinney method. The results of this risk analysis lead to objectives and measures to manage these risks.

The ISMS is based on the control measures mentioned in appendix Annex A of NEN ISO/IEC 27001. All parts of Annex A have been assessed on the information security risks for the organization, its employees, its products and services, customers, suppliers and other stakeholders. Control measures have been taken for each part in Annex A for which information security risks are recognized or for which information security risks are possible. In the Declaration of Applicability, which is based on the Annex A ISO 27001, the applicability of all parts has been indicated.

The management hereby declares that a management system is functioning within the organization that meets the requirements formulated in NEN ISO/IEC 27001.

The Hague, May 15, 2022

J. Linssen
CEO