Information and Privacy Security Policy

Objectives Information and privacy security

As Management of CSi, we attach great value to good information security, for the benefit of our customers, our employees and all external parties we work with.
We strive to ensure that all information that we collect, produce, exchange and store is adequately secured. Our information security policy is aimed at protecting the data we use as well as possible.

To implement this policy, we will ensure:

- that data, both internal information and from third parties, is treated confidentially;
- that the integrity of the data is guaranteed;
- that our information systems are designed in such a way that they are sufficiently protected against risks;
- that we comply with laws and regulations in the field of data security and privacy;
- that the continuity of our services is guaranteed by maintaining an effective Business Continuity Plan (BCP);
- that employees are sufficiently aware of the importance of good information and privacy security;
- that we take adequate measures to protect our information systems against unauthorised access and misuse.
- In addition to these requirements, we are bound by applicable laws and regulations (such as AVG).

With the documentation in our Information Security Management System (ISMS), which is set up in accordance with ISO/IEC 27001:2017, ISO/IEC27002:2017, we are in control and can demonstrate that we have mastered the matter and comply with legislation.

The organisation will strive for continuous improvement of the quality of information and privacy security. To this end, the effect of the control measures within the management system is regularly tested by means of self-assessments. Based on the findings, an activity plan is periodically drawn up in which the improvement measures are included.

Definition of Information and privacy security

Security is defined as follows:

"The coherent system of measures aimed at the permanent realisation of an optimal level of availability, integrity, confidentiality and privacy of information and information systems."
It is noted that information and privacy security comprises a coherent system of measures. This means that the various measures that together form information security are not separate from each other, but are mutually related.
The system of security measures aims to achieve a permanent high level of security. Careful safeguarding ensures that the desired level of security is also maintained in the long term. Information and privacy security is aimed at realising an optimal level of security. This optimum is achieved by careful consideration of the risks.

Information security and privacy objectives

As stated in the definition, information security focuses on the following aspects of information provision:

- availability, the information must be available at the desired times;
- integrity, the information must be correct and complete and the information systems must store and process correct and complete information;
- confidentiality, the information must only be accessible to those who are authorised;
- privacy, for information that contains (special) personal data high standards of confidentiality apply, including the measures chosen.

Concrete information and privacy security objectives are included in the ISMS action plan.

Responsibility for information and privacy security policy

The Management (Board) is ultimately responsible for the information security policy and has adopted this policy. CSi is aware that regular maintenance of the ISMS is necessary. Among other things, in the event of changes within the organisation, results of internal audits, risk assessments and developments in the field of legislation and regulations, the impact on the ISMS will be determined and corrective adjustments will be made.

Thus determined on 16th of September 2021
J.A.M. de Bruijn
CEO CSi Group