INFORMATION SECURITY MANAGEMENT SYSTEM POLICY - ISMS

PK 03

The information security management system (ISMS) is an integral part of the quality management system of SEP d.o.o. It is set in place so as to exploit the synergies with already established tools, such as risk assessment and management, supplier selection and evaluation and internal audit. By establishing the ISMS we step towards a systematic and comprehensive approach to information protection, which, however, does not mean that it was not already integrated in our operation. The following international standards serve as the basis for ISMS:

- TISAX VDA ISA 6.0
- ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements,
- ISO/IEC 27001:2022 Information technology – Security techniques – Code of practice for information security controls.

Here we also rely on other good practices and technological achievements in the area of information protection.

INFORMATION PROTECTION POLICY

The purpose of ISMS is to protect the information assets or the information system of the company against threats that may affect its integrity. Threats are identified as internal or external and intentional or unintentional. The integrity of the information system and information safety are key for the success and sustainability of our company's business operation. After all, this is also expected by our partners.

The success and sustainability of the company's operation are built on quality and trust, which are significantly affected by the safety of the information system and of the information. Its unauthorised disclosure, inaccessibility or even loss may directly harm the company commercially and lead to loss of reputation.

The company management supports and ensures sources for information protection.

The information protection policy of SEP d.o.o. includes:

- Categorising information assets based on the required level of protection.
- Protecting information against unauthorised access.
- Ensuring information confidentiality and integrity.
- Observing safety requirements with regard to employees.
- Managing physical and logical protection of information assets and premises.
- Observing legal and other regulations and contractual requirements.
- Observing the life cycle of systems in their development, implementation and maintenance.
- Ensuring business continuity.
- Regular informing all employees on the measures and novelties in the area of information protection.

- Managing incidents in the area of information protection.
- Sanctioning violations of the Information protection policy.

The Information protection policy is implemented with:

- Framework information protection policy which defines all key areas and is part of the IT process (NZP 7.0-01 IT),
- Instructions and processes.

They sensibly and in terms of each individual area define the roles, responsibilities and processes for:

- The company management,
- The persons responsible for information protection,
- Owners of data and processes,
- Technology suppliers and providers,
- Users,
- Internal auditors of information systems and
- Other possible stakeholders.

The person responsible for information protection is the IT administrator.

In accordance with adopted documents and commitments in the concluded contracts all employees and all interested parties are obliged to observe the information protection policy.

Date: 26/03/2025

Director:

Edmund Pal

Člani kolegija:

Tanja Jereb

Andrej Rajk

Brigita Borse

Janko Bahor

Darja Gregorčič Bernik

Branko Stojanović

Kristina Pevc

Jure Klenovšek

Vinko Zavratnik

VZ

Andrej Prevejšek

Branka Bradica