

ISMS POLICY

This information security management system (ISMS) policy is established by CEO to protect EYESEE from all types of internal and external unintentional or intentional threats, ensure business continuity, reduce risk levels, prevent security incidents and reduce their potential impact, protect the information assets against all internal, external, deliberate or accidental threats, and meet the needs and expectations of all relevant interested parties.

To raise awareness, the ISMS policy is communicated to all employees and other interested parties.

Prime principles of EYESEE business are based on market research by leveraging traditional and behavioral research methodologies such as eye-tracking, emotional recognition, virtual shopping, reaction time measurement, where is essential to satisfy applicable requirements related to the security of data.

The ISMS policy ensures commitment with the following:

- Protection against any unauthorized access and confidentiality of information gained from all relevant interested parties,
- Compliance with relevant legislative, regulatory, and contractual requirements, as well as other requirements applicable for EYESEE processes,
- Maintenance of information integrity, to be useful as needed,
- Developed, maintained, and tested business continuity plans, which assure continuity in process realization even in case of disasters,
- All actual or suspected information security breaches are reported and thoroughly investigated,
- Information security training available for all employees, in the onboarding phase and continuity during period of work,
- Continual improvement of information security management system, to be effective and appropriate to development in business processes of EYESEE.

The CEO has approved the ISMS policy and supports active acknowledgment of its values among all interested parties.

The Global Legal Lead is responsible for maintaining the policy and providing support and advice during its implementation.

All managers and process owners are responsible for implementing the policy and ensuring employee compliance in their processes.

Compliance with the ISMS policy is mandatory.

Signature:
CEO

Date: 06.08.2024.

DocuSigned by:

Joris De Bruyne

9438B2D2A21D478...