

COMPANY POLICY OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

The purpose of this policy is to establish a framework for ensuring the confidentiality, integrity, and availability of information processed by the company, including personal data transferred by our customers. By implementing, maintaining, and monitoring an Information Security Management System (ISMS) in accordance with the **ISO/IEC 27001** standard, we are committed to protecting our information and the information of our partners against loss, misuse, unauthorized access, leakage, or damage.

Scope

The ISMS covers all information systems, processes, employees, technologies, and data used in:

- providing printing and polygraphic services,
- processing print data and documents transferred by customers,
- storing personal data and other confidential information,
- managing internal documents, databases, and IT systems.

Information Security Principles

Confidentiality

We will ensure that information is accessible only to individuals who have authorized access, and is protected against unauthorized disclosure.

Integrity

We will ensure the accuracy, completeness, and consistency of information and its protection against unauthorized modification.

Availability

We will ensure that information and systems are available to authorized users in the required time and format.

Management Commitment

The company's management is committed to:

- fully supporting the established ISMS and providing the necessary resources for its maintenance and improvement,
- establishing and regularly reviewing information security objectives,
- promoting awareness and training for all employees in the area of ISMS,
- ensuring compliance with applicable legislation, standards, and contractual requirements (especially GDPR).

Processing of Personal Data

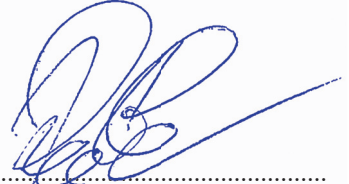
All personal data we obtain in the context of orders is processed strictly according to the customer's instructions and in compliance with the GDPR.

We commit to:

- protecting the transferred personal data throughout its processing,
- not storing it longer than strictly necessary,
- ensuring access to it only for authorized and trained personnel,
- timely addressing any security incidents involving personal data.

Employees and Responsibilities

Every employee is responsible for adhering to the ISMS rules and maintaining confidentiality. Access to confidential information is based on the „need to know“ principle. We regularly train employees in the areas of cybersecurity, GDPR, and handling confidential data.



.....
Managing Director
21. 07. 2025