

Information Security Policy – OptimiDoc s.r.o.

The objective of this policy is to define OptimiDoc s.r.o.'s commitment to protecting information assets, including data of our customers, partners, and other stakeholders, in accordance with the ISO/IEC 27001:2022 standard.

OptimiDoc s.r.o. commits to:

- Protecting the confidentiality, integrity, and availability of all information assets under its control.
- Complying with legal, regulatory, contractual, and industry security requirements, including GDPR, ISO/IEC 27001, and other cybersecurity frameworks.
- Applying risk management processes to identify, assess, and address risks threatening information assets.
- Ensuring business continuity through strong security measures and incident response procedures.
- Providing training and raising employee awareness about the importance of information security.
- Ensuring secure software development using proven methodologies and a secure development lifecycle.
- Protecting customer and partner data through secure design and secure deployment principles.
- Fulfilling legal and other requirements related to information security.
- Continuously improving the information security management system.

This policy applies to all employees, suppliers, and systems involved in the design, development, maintenance, operation, and support of software solutions for secure print management and document digitization, whether deployed in customer environments, partner environments, or public/private cloud environments.

All employees and contractual partners are expected to strictly adhere to this policy and report any identified or suspected information security incidents.

Approved by: Bronislav Šopík, CEO

Date: March 3, 2025

T: +420 576 880 059
E: info@optimidoc.com
W: www.optimidoc.com

A: tř. Tomáše Bati 385
763 02 Zlín
Czech Republic
VAT: CZ29294258

Registered in the Commercial Register maintained by the Regional Court in Brno, Section C, Entry 71857