

Technical and Organisational Security Policy

External edition for clients and contractors - aligned with ISO/IEC 27002:2023

1. Introduction

The company applies ISO/IEC 27002:2023 guidance to maintain a high level of information security and meet legal and client requirements. This document summarises the implemented safeguards in a clear, client-facing form.

2. Scope

The controls apply to IT systems, correspondence management, data handling, electronic communications, document storage and processing, and cooperation with service providers.

3. Key safeguards

- Access management limited to authorised persons
- Regular backups in external environments
- Physical protection of equipment and data
- Documented incident response procedures
- Cloud protection aligned with ISO requirements and the GDPR
- Cooperation only with verified suppliers meeting security requirements

4. Systems and technologies

- COK: correspondence registration with SSL and authorised access
- nazwa.pl: hosting and scan archiving with backups, encryption and EU storage
- iBard (Comarch): document backups
- Microsoft 365: identity management and encryption
- Koyto.pl / Webd.pl: backup hosting under security standards

5. Audits and compliance

Processes and documentation are periodically audited against ISO 27001, ISO 22301 and GDPR requirements. Safeguards are tested, reviewed and updated.

6. Security commitment

We protect client data, train personnel and maintain incident-response readiness to preserve confidentiality, integrity and availability.

7. Contact

Security and compliance enquiries may be submitted through the contact page at <https://backofficeoutsourcing.es/contact/>.

Informational translation. In the event of any discrepancy, the Polish original prevails.