BackOffice Outsourcing Sp. z o.o.
04-036 Warsaw
Al. Stanów Zjednoczonych 72/12
KRS 0000470010
NIP 1132867570
REGON 146791818

EORI: **PL113286757000000**
GLN: **5909000891012**
UKE Register of Postal Operators: **B-00516**
e-Delivery: **AE:PL-38861-91008-BSUUT-28**
https://backofficeoutsourcing.es

Security Policy

BackOffice Outsourcing Sp. z o.o.
External version for clients and contractors
(compliant with ISO/IEC 27001:2023)

1. Purpose of the document

The purpose of this policy is to confirm the company's commitment to ensuring the security of information entrusted by customers, partners and other stakeholders. This document is a declaration of the application of organisational and technical measures to ensure compliance with the requirements of ISO/IEC 27001:2023, and also with the law, in particular with regard to the protection of personal data (GDPR).

2. Scope

The policy covers all processes and resources related to the handling of customer information, in particular in the following services: correspondence and records management, data recording and digitisation, electronic archiving, operation of external systems and cloud infrastructure. The policy applies to all employees, collaborators and third parties entrusted with information processing.

3. General principles

- Customer information is processed with confidentiality, integrity and accessibility only to authorised persons.
- The company applies physical, logical and procedural security measures - in accordance with ISO/IEC 27001.
- Personal data is processed in accordance with Regulation (EU) 2016/679 (GDPR).
- All security incidents are promptly analysed and reported in accordance with established procedure.
- External partners (e.g. IT providers, document shredding companies) operate on the basis of entrustment agreements and in accordance with the security policy.
- Access to data and systems is controlled, monitored and periodically reviewed.
- Backups are stored securely and tested for recoverability.

4. Information Security Management System

The company has implemented and maintains an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2023, which includes, among other things: assessing risks and their systematic mitigation, setting security objectives, conducting audits and management reviews, corrective and preventive actions, training and staff awareness campaigns.

5. duties and responsibilities

Any person acting on behalf of the company or under its authority is required to comply with this policy. The implementation of the policy is overseen by a designated information security team acting in accordance with the internal documentation of the ISMS.

6. Information security contact

Anyone interested in the details of the data processing rules, the scope of delegated authority or the reporting of an incident can contact the designated Information Security Unit via the dedicated email address indicated in the contract or on the company's website.

7. Final provisions

This policy may be made available to clients and customers as evidence of the company's systematic approach to information protection and compliance with international security standards. The policy is subject to periodic review and update, at least once a year.