# Information Security Policy

Mailbutler GmbH

## 1 Purpose and Scope

This top-level Information Security Policy defines the framework for managing information security within Mailbutler GmbH, in alignment with the strategic direction of the organization and in accordance with information security standards following ISO 27001:2022.
The purpose of this Information Security Policy is to define a comprehensive framework for safeguarding Mailbutler GmbH's sensitive information, infrastructure, and reputation.

This policy is applied to the entire Information Security Management System (ISMS) as defined in the ISMS Manual.

## 2 Applicability

This policy applies to all employees, contractors, third-party service providers, and stakeholders who have access to Mailbutler GmbH's information assets or are involved in the management and protection of these assets. It encompasses all systems, networks, and data under the control of Mailbutler GmbH, irrespective of their location or form.

## 3 Policy Statement

Mailbutler GmbH is committed to safeguarding its information assets against all threats, whether internal or external, deliberate or accidental. Our Information Security Policy is founded on the following principles:

- **Purpose Alignment**: The policy is designed to support the mission and strategic goals of Mailbutler GmbH.
- **Information Security Objectives**: The policy provides a framework for setting, reviewing, and achieving information security objectives that are aligned with the organization's overall business objectives.
    - The general objectives of the information security management system are to ensure the confidentiality, integrity, and availability (CIA) of information assets,

thereby protecting the organization's reputation, legal standing, and operational effectiveness.
    - Top Management of Mailbutler GmbH is responsible for reviewing these general ISMS objectives and for defining new objectives.
    - Action targets for individual security measures or groups of security measures are defined in the ISMS Manual document. All these targets must be reviewed at least once a year.
    - Mailbutler GmbH evaluates and measures the achievement of these targets.

- **Information Security Controls**: The process for applying security controls is defined in the methodology for risk assessment and risk treatment. The selected controls and their implementation status are listed in the Statement of Applicability.
- **Legal and Regulatory Compliance**: Mailbutler GmbH is committed to complying with all applicable legal, regulatory, and contractual requirements related to information security. A detailed list of all contractual and legal requirements is provided with the list of legal, official, contractual, and other requirements.
- **Continuous Improvement**: We are dedicated to the ongoing enhancement of our ISMS, ensuring that it remains effective in the face of evolving threats and business changes.

# 4 Leadership and Commitment

Top management at Mailbutler GmbH is fully committed to establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS). This commitment is demonstrated by:

- **Strategic Alignment**: Ensuring that the information security policy and objectives are in line with the organization's overall strategic goals.
- **Integration**: Embedding information security requirements into all organizational processes, ensuring a holistic approach to risk management.
- **Resource Allocation**: Providing the necessary resources, including financial, technical, and human, to support the ISMS and achieve its intended outcomes.
- **Communication**: Actively promoting the importance of effective information security management and ensuring that all employees understand and adhere to the ISMS requirements.
- **Outcome Achievement**: Regularly reviewing the ISMS to ensure it meets its objectives and contributes to the overall security posture of the organization.

- **Support and Direction**: Encouraging and training all employees and relevant stakeholders to contribute to the effectiveness of the ISMS, fostering a culture of security awareness.
- **Continuous Improvement**: Championing initiatives that drive continuous improvement in the organization's information security practices.
- **Leadership in Roles**: Empowering other management roles within the organization to lead and demonstrate a commitment to information security within their respective areas of responsibility. Roles and responsibilities within the ISMS are defined in the *ISMS Manual* document.

For ensuring that the ISMS fulfils the requirements of this document, for coordinating the operation of the ISMS and for regularly reporting the effectiveness of the ISMS, top management appoints an Information Security Officer (ISO).

# 5 Documentation and Communication

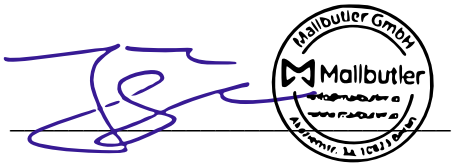
To ensure that this policy is effectively implemented, Mailbutler GmbH will:

- **Documentation**: Maintain this policy as documented information, ensuring it is regularly reviewed and updated to reflect any changes in the organization or the external environment.
- **Internal Communication**: Communicate this policy across all levels of the organization, ensuring that employees are aware of their roles and responsibilities in supporting the ISMS.
- **External Availability**: Make this policy available to interested parties, such as customers, partners, and regulators, as appropriate.

# 6 Review and Improvement

This Information Security Policy will be reviewed annually or as required to ensure its continued relevance and effectiveness. Feedback from internal audits, risk assessments, and incidents will be used to drive improvements in the ISMS and the overall security posture of the organization.

Berlin, July 21st, 2025




Information Security Officer