# Email Security Procedure Template

## Introduction

This Email Security Procedure outlines the guidelines and measures for ensuring the secure use of email systems within the organization. Aligned with ISO 27001 standards, this document provides a structured approach to mitigate risks associated with email communication, protect sensitive information, and maintain compliance with applicable regulations.

## Purpose

The purpose of this procedure is to establish a standardized framework for email security to safeguard the organization’s data, prevent unauthorized access, and protect against cyber threats such as phishing, malware, and data leaks. This ensures the confidentiality, integrity, and availability of information transmitted via email.

## Scope

This procedure applies to all employees, contractors, and third-party service providers who have access to the organization’s email systems. It encompasses all email communications sent, received, or stored using organizational resources.

## Policy Statement

1. Access Control: Only authorized personnel are granted access to organizational email accounts. Multi-factor authentication (MFA) must be enabled for all accounts.  
2. Email Content: Emails containing sensitive or confidential information must be encrypted before transmission using Advanced Encryption Standard (AES) with a minimum key length of 256 bits or other approved encryption tools specified by the IT Security Team.  
3. Phishing Awareness: Users must undergo regular training to recognize phishing attempts and report suspicious emails to the IT security team immediately.  
4. Attachment Security: All attachments received via email are subject to automated scanning for malware or other malicious content.  
5. Email Retention: Emails must be retained or deleted according to the organization’s data retention policy.  
6. External Email Communication: Restrictions apply to sharing sensitive information with external recipients, requiring prior approval and encryption mechanisms.

## Roles and Responsibilities

- Employees: Adhere to this procedure and report any security incidents involving email systems.  
- IT Security Team: Implement and manage email security tools, conduct regular monitoring, and provide training.  
- Management: Ensure adherence to the procedure and facilitate compliance among team members.  
- Compliance Officer: Oversee alignment with ISO 27001 and conduct periodic audits of email security practices.

## Compliance and Monitoring

Compliance with this procedure will be monitored through:  
- Regular audits of email security practices.  
- Automated alerts for unauthorized access or suspicious activities.  
- Periodic reviews of email logs to identify and address potential risks.  
Non-compliance will result in disciplinary actions as outlined in the organization’s policies.

## Related Documentation

- Information Security Policy  
- Data Classification Policy  
- Acceptable Use Policy  
- Incident Management Procedure

## Review and Revision

This procedure will be reviewed regularly or whenever significant changes occur in the organizational email system, threat landscape, or regulatory requirements. Revisions will be approved by the Information Security Steering Committee.

## Narrative Guidance

This document reflects the organization’s commitment to implementing ISO 27001. Adherence ensures the organization can prevent, detect, and respond to email-related threats effectively while fostering a culture of security awareness.