# Email Security Policy Template

## Document Control Information

- **Document Title:** Email Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

## 1. Introduction

### 1.1 Purpose

This Email Security Policy establishes [ORGANIZATION NAME]'s requirements for the secure use, management, and protection of email systems and communications in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that email is used securely and appropriately to protect organizational information.

### 1.2 Scope

This policy applies to: - All email systems owned, operated, or managed by [ORGANIZATION NAME] - All email communications sent or received using organizational email systems - All users of organizational email systems, including employees, contractors, consultants, and third parties - All devices used to access organizational email systems - All locations from which organizational email systems are accessed

### 1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing appropriate security controls for email systems - Protecting the confidentiality, integrity, and availability of email communications - Preventing unauthorized access to email systems and content - Defending against email-based threats and attacks - Ensuring appropriate use of email systems - Complying with relevant legal, regulatory, and contractual requirements - Regularly reviewing and improving email security controls

# 2. Email System Security

## 2.1 Infrastructure Security

- Email infrastructure shall be securely configured and maintained
- Security controls shall include:
    - Secure server configurations
    - Network security controls
    - Access controls
    - Encryption
    - Monitoring and logging
- Infrastructure shall be regularly updated and patched
- Infrastructure shall be regularly assessed for vulnerabilities
- Infrastructure changes shall follow change management procedures
- Infrastructure security shall be regularly reviewed

## 2.2 Email Transmission Security

- Email transmission shall be secured
- Security controls shall include:
    - Transport Layer Security (TLS) for email transmission
    - Secure SMTP configurations
    - Email authentication mechanisms (SPF, DKIM, DMARC)
    - Secure access protocols (IMAPS, POP3S)
- Encryption shall be used for sensitive email content
- Transmission security shall be regularly tested
- Transmission security shall be monitored
- Transmission security shall be regularly reviewed

## 2.3 Email Storage Security

- Email storage shall be secured
- Security controls shall include:
    - Access controls
    - Encryption where appropriate
    - Backup and recovery
    - Retention controls
    - Archiving security
- Storage shall be protected from unauthorized access
- Storage shall be protected from data loss
- Storage security shall be regularly assessed
- Storage security shall be regularly reviewed

# 3. Email Authentication and Access Control

## 3.1 User Authentication

- Email system access shall require strong authentication
- Authentication shall include:
    - Strong passwords or passphrases
    - Multi-factor authentication where appropriate
    - Account lockout after failed attempts
    - Password expiration and history controls
- Authentication credentials shall be protected
- Authentication methods shall be regularly reviewed
- Authentication security shall be regularly assessed
- Authentication incidents shall be promptly addressed

## 3.2 Access Control

- Email system access shall be controlled
- Access control shall include:
    - Role-based access
    - Principle of least privilege
    - Regular access reviews
    - Prompt removal of access when no longer needed
- Administrative access shall have enhanced controls
- Access shall be logged and monitored
- Access control effectiveness shall be regularly assessed
- Access control shall be regularly reviewed

## 3.3 Mobile Access

- Mobile access to email shall be secured
- Security controls shall include:
    - Device authentication
    - Device encryption
    - Remote wipe capability
    - Application controls
- Mobile access shall follow the Mobile Device Policy
- Mobile access security shall be regularly assessed
- Mobile access shall be monitored
- Mobile access security shall be regularly reviewed

## 4. Email Threat Protection

### 4.1 Anti-Malware Protection

- Email systems shall be protected against malware
- Protection shall include:
  - Email content scanning
  - Attachment scanning
  - URL filtering
  - Sandbox analysis for suspicious content
- Malware definitions shall be kept current
- Protection effectiveness shall be regularly assessed
- Malware incidents shall be promptly addressed
- Protection capabilities shall be regularly reviewed

### 4.2 Anti-Spam Protection

- Email systems shall be protected against spam
- Protection shall include:
  - Content filtering
  - Sender reputation checking
  - Rate limiting
  - Quarantine capabilities
- Spam definitions shall be kept current
- Protection effectiveness shall be regularly assessed
- False positives shall be addressed
- Protection capabilities shall be regularly reviewed

### 4.3 Phishing Protection

- Email systems shall be protected against phishing
- Protection shall include:
  - Sender authentication (SPF, DKIM, DMARC)
  - Look-alike domain detection
  - Suspicious content analysis
  - User awareness training
- Phishing attempts shall be reported and analyzed
- Protection effectiveness shall be regularly assessed
- Phishing incidents shall be promptly addressed
- Protection capabilities shall be regularly reviewed

### 4.4 Data Loss Prevention

- Email systems shall include data loss prevention (DLP)
- DLP shall include:
  - Content inspection
  - Pattern matching
  - File type controls
  - Sender/recipient controls
- DLP policies shall be based on data classification
- DLP effectiveness shall be regularly assessed
- DLP incidents shall be investigated
- DLP capabilities shall be regularly reviewed

## 5. Email Content Security

### 5.1 Content Controls

- Email content shall be controlled based on security requirements
- Controls may include:
  - Attachment type restrictions
  - Size limitations
  - Content filtering
  - URL filtering
  - Disclaimer requirements
- Controls shall be documented and communicated
- Control effectiveness shall be regularly assessed
- Controls shall be regularly reviewed
- Control exceptions shall be documented and approved

### 5.2 Email Encryption

- Sensitive email content shall be encrypted
- Encryption requirements shall be based on data classification
- Encryption methods may include:
  - Transport encryption (TLS)
  - End-to-end encryption
  - Attachment encryption
  - Portal-based secure messaging
- Encryption requirements shall be documented and communicated
- Encryption effectiveness shall be regularly assessed
- Encryption shall be regularly reviewed
- Encryption exceptions shall be documented and approved

### 5.3 Digital Signatures

- Digital signatures shall be used where appropriate
- Signature usage shall include:
  - Authentication of sender
  - Non-repudiation of content
  - Integrity verification
- Signature requirements shall be documented and communicated
- Signature verification shall be performed
- Signature effectiveness shall be regularly assessed
- Signature usage shall be regularly reviewed

## 6. Email Retention and Archiving

### 6.1 Retention Requirements

- Email retention shall comply with legal, regulatory, and business requirements
- Retention requirements shall be documented
- Retention shall be consistently applied
- Retention shall be technically enforced where possible
- Retention compliance shall be regularly assessed
- Retention exceptions shall be documented and approved
- Retention requirements shall be regularly reviewed
- Retention shall align with the Records Management Policy

### 6.2 Archiving

- Email archiving shall be implemented
- Archiving shall include:
  - Secure storage
  - Search capabilities
  - Access controls
  - Integrity protection
  - Retention controls
- Archiving shall comply with legal and regulatory requirements
- Archive access shall be controlled and logged
- Archive security shall be regularly assessed
- Archiving effectiveness shall be regularly reviewed

### 6.3 Legal Hold

- Legal hold procedures shall be established for email

- Procedures shall include:
    - Hold implementation
    - Scope definition
    - Notification requirements
    - Preservation requirements
    - Hold release
- Legal holds shall override normal retention
- Legal hold compliance shall be monitored
- Legal hold procedures shall be regularly reviewed
- Legal hold shall be coordinated with legal counsel

## 7. Email Usage

### 7.1 Acceptable Use

- Email shall be used in accordance with the Acceptable Use Policy
- Acceptable use shall include:
    - Business purpose
    - Professional communication
    - Appropriate content
    - Resource conservation
- Prohibited use shall include:
    - Illegal activities
    - Harassment or offensive content
    - Unauthorized disclosure of information
    - Personal business
    - Impersonation
- Acceptable use shall be documented and communicated
- Acceptable use compliance shall be monitored
- Acceptable use violations shall be addressed

### 7.2 Personal Use

- Personal use of email shall be limited
- Personal use shall:
    - Not interfere with work duties
    - Not consume significant resources
    - Not expose the organization to risk
    - Not violate policies
- Personal use limitations shall be documented and communicated
- Personal use compliance shall be monitored
- Personal use violations shall be addressed

- Personal use policy shall be regularly reviewed

### 7.3 Email Disclaimers

- Email disclaimers shall be implemented
- Disclaimers shall include:
  - Confidentiality statement
  - Misdirected email instructions
  - Legal notices
  - Organization information
- Disclaimers shall be automatically applied
- Disclaimers shall comply with legal requirements
- Disclaimer effectiveness shall be regularly assessed
- Disclaimers shall be regularly reviewed

## 8. Email Security Practices

### 8.1 Email Handling

- Email shall be handled according to content sensitivity
- Handling shall include:
  - Appropriate addressing
  - Appropriate content
  - Attachment handling
  - Link handling
  - Forwarding controls
- Handling requirements shall be documented and communicated
- Handling compliance shall be monitored
- Handling violations shall be addressed
- Handling requirements shall be regularly reviewed

### 8.2 Distribution Lists

- Email distribution lists shall be controlled
- Controls shall include:
  - Creation approval
  - Membership management
  - Usage restrictions
  - Regular review
- Distribution list owners shall be assigned
- Distribution list security shall be regularly assessed
- Distribution list usage shall be monitored
- Distribution list controls shall be regularly reviewed

### 8.3 Auto-Forwarding

- Email auto-forwarding shall be controlled
- Controls shall include:
    - Restrictions on external forwarding
    - Approval requirements
    - Monitoring and logging
    - Regular review
- Auto-forwarding shall comply with data protection requirements
- Auto-forwarding security shall be regularly assessed
- Auto-forwarding usage shall be monitored
- Auto-forwarding controls shall be regularly reviewed

### 8.4 Out-of-Office Messages

- Out-of-office messages shall be controlled
- Controls shall include:
    - Content restrictions
    - Distribution restrictions
    - Duration limitations
    - Security considerations
- Out-of-office requirements shall be documented and communicated
- Out-of-office compliance shall be monitored
- Out-of-office security shall be regularly assessed
- Out-of-office controls shall be regularly reviewed

## 9. Email Security Incidents

### 9.1 Incident Types

Email security incidents may include: - Unauthorized access - Data breaches - Malware infections - Phishing attacks - Spam campaigns - Data loss - Policy violations - System compromises

### 9.2 Incident Response

- Email security incidents shall be managed according to the Incident Management Policy
- Response shall include:
    - Incident detection
    - Incident reporting
    - Incident containment
    - Incident investigation

    - Incident remediation
    - Incident documentation
- Response procedures shall be documented
- Response effectiveness shall be regularly assessed
- Response capabilities shall be regularly tested
- Response lessons learned shall be incorporated into controls

### 9.3 Incident Reporting

- Email security incidents shall be promptly reported
- Reporting shall include:
    - Incident description
    - Systems affected
    - Users affected
    - Data affected
    - Actions taken
- Reporting procedures shall be documented and communicated
- Reporting shall be to appropriate personnel
- Reporting effectiveness shall be regularly assessed
- Reporting shall comply with legal and regulatory requirements

## 10. Monitoring and Compliance

### 10.1 Email Monitoring

- Email systems shall be monitored for security purposes
- Monitoring shall include:
    - System performance
    - Security events
    - User activities
    - Policy compliance
- Monitoring shall respect privacy requirements
- Monitoring shall be documented and communicated
- Monitoring effectiveness shall be regularly assessed
- Monitoring shall be regularly reviewed

### 10.2 Logging Requirements

- Email system activities shall be logged
- Logs shall include:
    - Authentication events
    - Access attempts
    - System changes

  - Security events
  - User activities
- Logs shall be protected from tampering
- Logs shall be retained according to requirements
- Logs shall be regularly reviewed
- Log anomalies shall be investigated

### 10.3 Compliance Verification

- Email security compliance shall be regularly verified
- Verification may include:
  - Self-assessments
  - Internal audits
  - External audits
  - Technical testing
- Verification results shall be documented
- Non-compliance shall be addressed
- Verification effectiveness shall be regularly assessed
- Verification shall be regularly reviewed

## 11. Training and Awareness

### 11.1 User Training

- Email users shall receive security training
- Training shall cover:
  - Email security threats
  - Security best practices
  - Policy requirements
  - Incident reporting
  - Handling sensitive information
- Training shall be provided at onboarding and regularly thereafter
- Training completion shall be documented
- Training effectiveness shall be assessed
- Training materials shall be regularly updated

### 11.2 Security Awareness

- Email security awareness shall be maintained
- Awareness activities may include:
  - Regular communications
  - Security alerts
  - Phishing simulations

    - Security tips
    - Incident lessons learned
- Awareness shall address current threats
- Awareness effectiveness shall be assessed
- Awareness materials shall be regularly updated
- Awareness shall be integrated into organizational culture

## 12. Third-Party Email Services

### 12.1 Service Requirements

- Third-party email services shall meet security requirements
- Requirements shall include:
    - Security controls
    - Compliance capabilities
    - Service level agreements
    - Data protection
    - Incident response
- Requirements shall be documented in contracts
- Service security shall be regularly assessed
- Service compliance shall be regularly verified
- Service security incidents shall be promptly addressed

### 12.2 Cloud Email Security

- Cloud email services shall be secured
- Security shall include:
    - Access controls
    - Data protection
    - Encryption
    - Backup and recovery
    - Compliance capabilities
- Cloud security shall be regularly assessed
- Cloud security compliance shall be regularly verified
- Cloud security incidents shall be promptly addressed
- Cloud security shall align with the Cloud Security Policy

## 13. Roles and Responsibilities

### 13.1 Management

- Approve email security policy

- Provide resources for email security
- Review email security performance
- Address significant email security issues
- Support email security initiatives
- Ensure compliance with requirements
- Approve risk acceptance when necessary

### 13.2 Information Security Team

- Develop and maintain email security policy
- Define email security requirements
- Review email security controls
- Monitor email security compliance
- Investigate email security incidents
- Provide security guidance and expertise
- Report on email security status

### 13.3 IT Department

- Implement email security controls
- Manage email systems and infrastructure
- Monitor email operations
- Support email users
- Implement security updates and patches
- Respond to technical incidents
- Report on email operational status

### 13.4 All Users

- Comply with email security policy
- Use email securely and appropriately
- Report security incidents and concerns
- Complete required training
- Follow security best practices
- Protect sensitive information
- Support security initiatives

## 14. Compliance and Exceptions

### 14.1 Compliance Monitoring

- Email security compliance shall be regularly monitored

- Monitoring shall include:
    - Policy compliance
    - Technical controls
    - User behavior
    - Security incidents
- Non-compliance shall be addressed
- Compliance trends shall be analyzed
- Compliance reports shall be provided to management
- Compliance monitoring shall be regularly reviewed

### 14.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate - Tracked and reported - Minimized to the extent possible - Consistent with legal and regulatory requirements

## 15. Related Documents

- Information Security Policy
- Acceptable Use Policy
- Data Classification Policy
- Incident Management Policy
- Records Management Policy
- Mobile Device Policy
- Cloud Security Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

## 16. Approval

This Email Security Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________