

Email Security Policy Template

A free, adaptable template covering scope, technical controls (SPF, DKIM, DMARC, MFA), sensitive data, phishing reports, payment-change verification, retention, and the evidence auditors sample. Mapped to SOC 2, ISO 27001, HIPAA, and PCI DSS.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with your own. Delete any section that does not apply, keep the numbering, and route the final version through your normal approval process. The values are recommended defaults, not framework requirements: SOC 2, ISO 27001, and HIPAA name no email-specific settings, PCI DSS 4.0.1 Requirement 5.4.1 requires anti-phishing mechanisms, and Google sets sender thresholds for mail sent to personal Gmail accounts. Write rules you can show evidence for every month.

Company: [Company name] _____

Policy owner: [Role, e.g. Security Lead] _____

Version: [1.0] _____

Effective date: [Date] _____

Approved by: [Name, title] _____

Next review: [Date, at least annually] _____

1. Purpose and scope

Purpose. This policy defines how [Company] protects its email and messaging, what may be sent and received, how suspected phishing is reported, and how payment requests are verified, so that information is protected in transit and every exception is recorded.

Scope. This policy applies to all employees, contractors, and third parties who use any of the following:

- Company mailboxes on [Google Workspace / Microsoft 365]
- Shared mailboxes and aliases (for example support@ and billing@)
- Mail sent as a [Company] domain by any tool, including marketing, support, billing, and product notification services
- Chat and messaging platforms such as [Slack / Teams] and SMS

Out of scope. Personal email accounts. They must not be used for company data (see section 5).

Related policies. Acceptable Use Policy, Security Awareness Training Policy, Data Classification Policy, Data Encryption Policy, Data Retention Policy, Incident Management Policy.

2. Roles and responsibilities

Role	Responsibility
Policy owner [Security Lead]	Owns this policy, approves exceptions, reviews DMARC reports and the monthly summary
Mail administrator [IT lead]	Maintains DNS records, admin console settings, filtering, and retention settings
Sender owners	Each tool that sends as a company domain has a named owner who keeps its authentication current
Finance and approvers	Apply the payment-change verification rule in section 7
All personnel	Follow this policy, complete awareness training, and report suspected phishing

3. Account and access rules

- Every mailbox requires multi-factor authentication. Administrator accounts use phishing-resistant methods where available.
- Legacy authentication protocols are disabled.
- Automatic forwarding to external addresses is blocked. Exceptions require written approval from the policy owner.
- The company owns all mailboxes and their contents. Messages may be reviewed for security and legal purposes, and personnel are notified of this in writing.
- Shared mailboxes have a named owner and an access list reviewed [quarterly].
- On departure, the mailbox is suspended, forwarding is checked, and delegated access is removed on the last working day.

4. Technical controls

Control	Requirement
SPF	Published for every company domain. Lists only approved sending services.
DKIM	Enabled for the mail platform and for every tool that sends as a company domain.
DMARC	Published for every company domain. Moves from monitoring (none) to quarantine to reject within [6] months of adoption. Aggregate reports reviewed [weekly] until at reject, then [monthly].
TLS	Required for mail in transit.
Filtering	Inbound filtering and attachment scanning are enabled and must not be disabled. Risky attachment types ([executables, macro-enabled files]) are blocked.
External warning	Messages from outside the company display a visible external-sender notice.

Sender inventory	The policy owner keeps a list of every tool allowed to send as a company domain, with its owner. Product notifications use a dedicated subdomain.
-------------------------	---

5. Data handling and encryption

Data class	Email rule
Public	May be sent freely.
Internal	Company accounts only. Never to personal addresses.
Confidential	Encrypted transmission, verified recipient, no forwarding outside the intended group.
Restricted	Do not email. Use [approved secure sharing tool] with access controls and expiry.

- Passwords, API keys, and recovery codes are never sent by email.
- Company data is never sent to or stored in personal email accounts.
- Check the recipient list before sending anything classified Confidential or higher.
- A misdirected message is reported immediately as a security event under the Incident Management Policy.

6. Phishing reporting

- **Where to report:** [report-phishing button / alias].
- **Acknowledgement:** the policy owner confirms receipt within [1 business day] and tells the reporter what to do with the message.
- **No blame:** a person who clicked and reports immediately is not disciplined. Response is credential reset and review.
- **Close-out:** the owner records the report, removes the message from other mailboxes, and notes whether anyone else interacted with it.

7. Payment-change verification (business email compromise)

1. Treat every change to payment details as unverified, whoever it appears to come from.
2. Verify by calling a number already on file, never one given in the message.
3. A second authorized approver is required for any change and for any payment above [threshold].
4. Do not confirm a change by replying to the original thread.
5. Record the verification, including who was spoken to, in the payment ticket.
6. The same rule applies to urgent requests that appear to come from executives, including gift cards and confidential transfers.

8. Retention and monitoring

The default retention period for email is [36] months, set in the data retention policy and applied by a mail platform setting. Legal holds suspend deletion automatically when litigation or an investigation is likely. Access to search and export mail is limited to [named roles] and logged. Monitoring is performed for security and legal purposes only. [Have counsel review this section for your jurisdictions.] No framework sets an email retention period: choose the value from your contractual, legal, and privacy obligations.

9. Evidence and review

Keep the following records for at least [the audit period plus one year]. Review this policy at least annually and after any change in the mail platform.

Evidence	What it shows
Approved policy and version history	The rules exist and someone with authority signed off
SPF, DKIM, and DMARC DNS records	Authentication is published and enforced
DMARC aggregate reports	Unauthorized senders are being watched
MFA enforcement report	Every mailbox is covered
Admin console settings (dated)	Forwarding and legacy authentication are off
Phishing report tickets	Reports are triaged and closed
Payment-change verification records	The callback rule was followed
Policy acknowledgements	Personnel were told the rules

Framework notes

Framework	Where it lives	What it says about email
SOC 2	CC6.7, CC6.8	No email-specific setting named. Transmission protection and malicious software controls are evidence. Auditors test against your own policy.
ISO 27001:2022	Annex A 5.14, 6.8, 8.12	Information transfer (including electronic messaging), event reporting, data leakage prevention. Selected through the Statement of Applicability.
HIPAA	45 CFR 164.312(e)	Transmission security is required. Integrity controls and encryption are addressable.
PCI DSS 4.0.1	Requirement 5.4.1	Processes and automated mechanisms to detect and protect personnel against phishing. Mandatory after March 31, 2025.

CIS Controls v8	Safeguard 9.5	Implement DMARC (implementation groups 2 and 3).
Google sender guidelines	Since Feb 1, 2024	SPF or DKIM, TLS, spam rate below 0.3% for mail to personal Gmail accounts. Senders of 5,000+ messages a day also need SPF, DKIM, DMARC, and one-click unsubscribe on marketing mail.

Free template by [ComplyJet](#). Read the full guide at complyjet.com/blog/email-security-policy-template. This template is a starting point, not legal or audit advice. Adapt it to your environment and have it reviewed before adopting.