This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

# Email Protection Standard Template

Choose Classification

| | |
|---|---|
| DATE | Click here to add date |
| VERSION | Click here to add text |
| REF | Click here to add text |

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press "Ctrl" + "H" keys simultaneously.
- Enter "<organization name>" in the Find text box.
- Enter your organization's full name in the "Replace" text box.
- Click "More", and make sure "Match case" is ticked.
- Click "Replace All".
- Close the dialog box.

# Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

# Document Approval

| Role | Job Title | Name | Date | Signature |
|---|---|---|---|---|
| Choose Role | <Insert job title> | <Insert individual's full personnel name> | Click here to add date | <Insert signature> |
| | | | | |

# Version Control

| Version | Date | Updated By | Version Details |
|---|---|---|---|
| <Insert version number> | Click here to add date | <Insert individual's full personnel name> | <Insert description of the version> |
| | | | |

# Review Table

| Periodical Review Rate | Last Review Date | Upcoming Review Date |
|---|---|---|
| <Once a year> | Click here to add date | Click here to add date |
| | | |

# Table of Contents

# Purpose

This standard aims to define the detailed cybersecurity requirements related to <organization's name>'s email in order to minimize cybersecurity risks resulting from internal and external threats at <organization's name>.

The requirements in this standard are aligned with the Email Protection Policy and the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

# Scope

This standard covers all <organization name>'s information and technology assets (including email systems) and applies to all personnel (employees and contractors) in <organization name>.

# Standards

| 1 | Content Filtering and Analysis |
|---|---|
| Objective | To ensure the protection of email addresses from spam email messages, phishing email messages, malicious Uniform Resource Locators (URLs), and any other type of harmful content. |
| Risk Implication | Users may be deceived by email messages that contain malicious and suspicious content, and <organization name> may be exposed to cyberattacks if email messages are not checked and verified. |
| Requirements | |
| 1-1 | All <organization name>'s inbound and outbound email messages must be scanned for malicious and suspicious content. |

| | |
|---|---|
| 1-2 | All <organization name>'s inbound and outbound email messages must be labeled with appropriate protective labeling reflecting the sensitivity and confidentiality levels based on the data classification level and as per <organization name>'s Data Classification Policy and the results of content analysis. Alternatively, <organization name>'s applicable Labeling Standard must be used as per <organization name>'s Email Protection Policy. Some examples of labels are: safe, sensitive, etc. |
| 1-3 | All <organization name>'s inbound and outbound email messages must be tagged with appropriate protective tagging reflecting the sensitivity and confidentiality levels based on the data classification level and as per <organization name>'s Data Classification Policy and the results of content analysis. Alternatively, <organization name>'s applicable Tagging Standard must be used as per <organization name>'s Email Protection Policy. Some examples of tags are malicious, bad sender, inappropriate, spam, suspected spam, etc. |
| 1-4 | All inbound email messages must be blocked and tagged/labeled to reflect disallowed content as per <organization name>'s Email Protection Policy. For example:<br>• **Block** malicious, blacklisted and spam email messages.<br>• **Quarantine** suspected spam email messages.<br>• **Allow** safe email messages. |
| 1-5 | All outbound classified email messages must be blocked based on the protective tags/labels reflecting the email classification level as per <organization name>'s Email Protection Policy. For example:<br>• **Block** sensitive and confidential email messages.<br>• **Allow** public and restricted email messages. |

| | |
|---|---|
| 1-6 | Spam email messages reflecting unacceptable spam risk scores must be blocked as per <organization name>'s Email Protection Policy. For example:<br>• **Block** high risk email messages.<br>• **Quarantine (block the message until making sure it is safe)** medium risk email messages .<br>• **Allow** low risk and no-risk email messages. |
| 1-7 | Inbound email messages containing malicious URLs, phishing attempts, malicious domains, etc. must be blocked. |
| 1-8 | Active Web Addresses in email messages must be replaced with other addresses. |
| 1-9 | Inbound email messages containing active content must be blocked. Alternatively, the active content in the email's body must be removed. |
| 1-10 | Inbound and outbound email messages with extra-large files or content, or with unapproved file format or extension must be blocked according to <organization name>'s policy or delayed until the files are verified by the responsible employee or as per the enforced policy. |
| 1-11 | Outbound email messages to unknown distribution lists must be blocked. |
| 2 | Secure Authentication |
| Objective | To ensure the protection of email from unauthorized access from outside <organization name> through webmail or an email client. |

| | |
|---|---|
| Risk Implication | Unauthorized access to email exposes <organization name> to major risks that can lead to information theft and impersonation, which can be used to carry out further cybersecurity attacks against <organization name> and its infrastructure. |
| Requirements | |
| 2-1 | Multi-Factor Authentication (MFA) must be implemented for remote email client access, webmail access by users (e.g., Outlook Web Access "OWA") and mobile applications. |
| 2-2 | Besides a user/password combination, <organization name> must implement other authentication mechanisms when accessing email messages from outside the network (e.g., biometrics, hardware keys, one-time passwords). |
| 2-3 | Complex email password requirements must be configured as per <organization name>'s Identity and Access Management Policy. |
| 2-4 | Encryption methods, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), must be implemented to protect authentication mechanisms during transmission. Recommended next generation encryption protocols and cipher suites (such as cipher suite B) must be used as per <organization name>'s approved Cryptography Standard and National Cryptographic Standards. |
| 3 | Content Protection |
| Objective | To ensure that email messages that contain attachments are protected against viruses, malware, Advanced Persistent Threats (APTs), Zero-Day attacks, and any other type of malicious attachments. |
| Risk implication | Users may be deceived by email messages that contain malicious attachments, and <organization name> may be |

| | |
|---|---|
| | exposed to a data breach, unauthorized access, or unauthorized disclosure if email attachments are not checked. |
| Requirements | |
| 3-1 | Two types of email attachment classification must be configured; based on file type and based on file content. |
| 3-2 | Attachments based on file types and formats must be tagged. For example:<br>• **Blacklist:** All forms of Windows PE, Office macros, scripts, etc.<br>• **Graylist (quarantine-list):** Multi-layer archives, password protection files, encryption files, files exceeding the maximum size, and other files that are included in quarantine-list.<br>• **Whitelist:** Standard Microsoft Office extensions (docx, pptx, xlsx, etc.), pdf, txt, archives, etc.<br>• **Unknown:** Unknown file type/format, or unable to detect**.** |
| 3-3 | All malware-scanned attachments must be tagged with scan results. For example:<br>• **Malicious:** Contains virus, malware, APT, etc.<br>• **Safe:** Malware-free attachment.<br>• **Unknown:** Unable to scan. |
| 3-4 | File types must be determined using file content (file header and footer), not extensions. |
| 3-5 | All whitelisted and filtered attachments must be scanned for malicious files including viruses, malware, and any other form of suspicious files. |
| 3-6 | Malware scanning must be performed on Mail Gateway, Mail Relay or Mail Server before it reaches the Email Client. |

| | |
|---|---|
| 3-7 | Malware scanning must be performed on email clients using a solution from a vendor or provider different from the one mentioned in clause 3-6 (e.g., AV plug-ins added to outlook client) |
| 3-8 | Allowed attachments, on which dynamic analysis was performed in sandbox, must be scanned to detect Advanced Persistent Threats (APTs) and Zero-Day malware. |
| 3-9 | All email messages with blacklisted or malicious attachments must be blocked/stripped as per <organization name>'s Email Protection Policy. Sender's email address and domain must be added to the blacklist. |
| 3-10 | All email messages with graylisted attachments must be quarantined if they are malware-free. |
| 3-11 | All email messages with **Unknown** attachments must be quarantined. |
| 3-12 | All email messages with whitelisted attachments must be allowed if they are malware-free. |
| 4 | Email Sender Verification |
| Objective | To ensure the confidentiality of email data and verify their integrity and reliability to protect it against unauthorized access and critical information disclosure. |
| Risk implication | Verifying the integrity and reliability of email messages protects <organization name> against email fraud, malicious email messages, critical and sensitive information disclosure, and unauthorized access to user's email messages. |
| Requirements | |
| 4-1 | Sender must be verified against at least two sender reputation databases. |

| | |
|---|---|
| 4-2 | Sender email address must be verified against sender spam lists that are available on the Internet and are updated daily. |
| 4-3 | Sender email server **IP** and **domain name** must be verified against Real-time Blackhole Lists (RBL). |
| 5 | Email Chain of Trust Verification |
| Objective | To ensure the confidentiality of email data and verify their integrity and reliability to protect them against unauthorized access and critical information disclosure. |
| Risk implication | Failing to verify the integrity and reliability of email messages can lead to email fraud, malicious email messages, critical and sensitive information disclosure, and unauthorized access to user email messages. |
| Requirements | |
| 5-1 | Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) must be created and registered. |
| 5-2 | Senders must be verified according to their Sender ID/SPF records and actions must be taken as per <organization name>'s Email Protection Policy.<br>• **Reject** SPF hard-fail<br>• **Quarantine** SPF soft-fail |
| 5-3 | Senders must be verified according to their DKIM.<br>• **Reject** DKIM fail. |
| 5-4 | SPF on external records facing DNS must be configured for each and every domain name owned by <organization name> to allow only Mail Exchange Records (MX Records) of servers authorized by <organization name> to send email messages on its behalf. |
| 5-5 | DKIM records must be configured to sign the content of <organization name>'s email messages by specifying cryptographic public keys for signing. |
| 5-6 | Domain-based Message Authentication, Reporting and Conformance (DMARC) must be configured to automate the |

| | |
|---|---|
| | actions taken on Sender ID/SPF fails and DKIM fails according to the email security policy of <organization name>. For example:<br>• **Reject/Quarantine** Relaxed Fail in DKIM and SPF.<br>Note: Relaxed Fail allows email messages received from sub-domains and Strict Fail blocks them. |
| 6 | Email Systems Security |
| Objective | To ensure the protection and security of email service infrastructure including email servers, gateway, databases, and security solutions. |
| Risk implication | Failing to take any measures to protect email service infrastructure in <organization name> can allow attackers to exploit weaknesses and vulnerabilities in email systems to gain unauthorized access to <organization name>'s network and data. |
| Requirements | |
| 6-1 | Regular security testing (such as vulnerability assessments and penetration testing) must be performed as per <organization name>'s relevant policies and procedures. |
| 6-2 | Email systems must be regularly patched and updated as per <organization name>'s Patch Management Policy. Additionally, it must be ensured that all systems are up-to-date. |
| 6-3 | Unnecessary/unrequired applications and services on email systems, such as printing services, telnet, etc. must be removed/disabled. |
| 6-4 | Secure Configuration and Hardening must be applied every three months on applications, databases, and operating systems. Refer to <organization name>'s Server Security Standard and Database Security Standard. |
| 6-5 | Access to email systems must be restricted to email system administrators only. |

| | |
|---|---|
| 6-6 | Default/non-interactive/unneeded accounts must be removed/disabled |
| 6-7 | Email systems administrators and operators must be obliged to use Multi-Factor authentication to access email systems. |
| 6-8 | The least-privilege principle must be used to provide access for email system administrators and operators to email systems. |
| 6-9 | Network access to email management systems must be restricted to Email System Zone and Management Zone. |
| 6-10 | Unnecessary/unrequired email application features and configuration files must be removed/disabled. |
| 6-11 | Access to unnecessary/unrequired network and file directories must be blocked. |
| 6-12 | Peripheral device controls must be used and access to removable media, such as CDs, DVDs, and USBs, must be blocked. |
| 6-13 | Email systems software must be installed on dedicated hosts. |
| 6-14 | The service banners of mail transport protocols (such as SMTP, POP, IMAP, etc.) must be configured to prevent software/protocol version disclosure (Exchange version). |
| 6-15 | Safe email commands must only be enabled to avoid risky email commands (such as VRFY and EXPN). |
| 6-16 | Email systems event logging and audit log to be forwarded to a centralized event logging system must be configured as per <organization name>'s approved Cybersecurity Event Logs and Monitoring Management Policy and Standard. |
| 6-17 | A Multi-Tier architecture protected by a dual layer of firewalls must be applied when creating the email service infrastructure, specifically, **Mail Gateway** in the Internet DMZ, |

| | |
|---|---|
| | **Email Application Servers** in the Production Zone, and **Email Database Servers** in the Trusted or Database zone. |
| 6-18 | The webmail page must be protected behind a web application firewall (WAF). |
| 6-19 | Open Mail Relay feature must be disabled. |
| 6-20 | Email transport encryption must be configured using encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), to protect email messages during transmission. Recommended next generation encryption protocols and cipher suites (such as cipher suite B) should be used as per <organization name>'s approved Cryptography Standard. |
| 6-21 | Activate STARTTLS technology to encrypt communication between e-mail email gateways to prevent passive man-in-the-middle attacks. |
| 6-22 | Mail bounce profiles must be configured, for example:<br>**Hard Bounce** for email messages sent to non-existing users or expired/disabled email addresses. |
| 7 | Email Client Security |
| Objective | To ensure the protection of email usage through webmail or an email client. |
| Risk implication | Failing to take any measures to protect email clients can cause serious risks that can lead to information theft and impersonation, which can be used to carry out malicious attacks against <organization name>'s personnel and infrastructure. |
| Requirements | |
| 7-1 | Only fully supported and up-to-date email clients must be used. |

| | |
|---|---|
| 7-2 | Running the webmail on unsupported browsers must be prohibited. |
| 7-3 | Unnecessary or not whitelisted email client plug-ins or add-ons applications must be disabled. |
| 7-4 | Running scripting languages in email clients must be prohibited. |
| 7-5 | Email clients must be integrated with end-point security products (e.g., AV and Malware). |
| 8 | Backup and Archival |
| Objective | To ensure the integrity, availability, and recoverability of email data and protect them against loss or damage. |
| Risk implication | If email data or email messages are deleted, tampered with, lost by mistake, corrupted, or subjected to a cybersecurity attack, <organization name> will not be able to recover its email data and communication records, which will impact its usual business operations. |
| Requirements | |
| 8-1 | Backup and archival for email messages must be implemented in accordance with the technical security controls mentioned in the Backup and Disaster Recovery Management standard applied in <organization name> in order to defend cybersecurity attacks. |

# Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function>
4- **Standard Compliance Measurement:** <cybersecurity function>

## Update and Review

<cybersecurity function> shall review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

## Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.
2- All employees at <organization name> shall comply with this standard.
3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.