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 outlined image.

Email Security Policy 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 policy aims to define the cybersecurity requirements related to the protection of <organization name>'s email to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

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

Scope

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

Policy Statements

1 General Requirements

1-1 The necessary technologies to protect the confidentiality, integrity, and availability of email messages during transmission and storage must be used and updated constantly.

1-2 Email protection, analysis, and filtering technologies must be used to block suspicious email messages, such as spam and phishing email messages.

1-3 The necessary technologies, such as Data Leakage Prevention (DLP), must be used to protect data against leakage via email from inside or outside <organization name>.

1-4 Technologies must be used to protect email servers against Advanced Persistent Threats (APTs) and zero-day malware.

1-5 Technologies must be used to inspect email message attachments and links in a sandbox before they reach the user's mailbox, whether such email messages are sent from inside or outside <organization name>.

1-6 Modern technologies must be used to ensure the reliability of <organization name>'s incoming email message domains, including but not limited to, using the email authentication service within the National Portal for Cybersecurity Services (Haseen), and applying Send Protection Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) verification protocols to prevent email spoofing.

1-7 The necessary technologies to encrypt email messages containing classified information must be used in accordance with <organization name>'s regulatory procedures and policies.

1-8 Multi-Factor Authentication (MFA) must be implemented for remote email access and webmail login.

1-9 Email messages must be archived and backed up periodically as per <organization name>'s approved and related regulatory procedures and policies.

1-10 Generic accounts' owners and their responsibilities must be identified.

1-11 Secure access to email messages must be implemented and restricted to <organization name>'s personnel only.

1-12 The necessary measures must be taken to prevent the use of <organization name>'s email for non-authorized business purposes.

1-13 The System Administrator must not be allowed to access any personnel's information and email messages without prior authorization and must follow defined and approved procedures.

1-14 The size and type of inbound and outbound email attachments and the capacity of the mailbox must be determined for each user. Sending group messages to many users must be limited.

1-15 Email messages sent to outside <organization name> must be appended with a disclaimer.

1-16 Email messages must be classified according to the criticality of their attachments and information in accordance with <organization name>'s approved Data and Information Classification Policy.

1-17 Open mail relay services must be disabled on the server.

1-18 The use of email must be prohibited for privileged accounts.

1-19 Connections between email gateways must be encrypted to prevent inactive man-in-the-middle attacks.

1-20 <cybersecurity function> must ensure the cybersecurity awareness of all personnel and educate them to handle secure email services and detect phishing emails.

1-21 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of email protection requirements.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

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

3- **Policy Implementation and Execution:** <information technology organization> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy 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- <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.