



Integrated Government Philippines Project

Filipino nation moving toward globally competitive ICT-empowered government



Information and Communications
Technology Office



Advanced Science
and Technology Institute

Prescribing theGovMailService Guidelines for Philippine Government Agencies



Overview

1. Purpose – Use, Awareness, Basis
2. Scope – Officials, All Communications/Features, all access devices
3. Policies
4. Roles and Responsibilities

Policies

A.Accounts

B.E-mail Naming Convention

C.Acceptable Use of theGovMailService

D.Prohibited Use of theGovMailService

E.Privacy and Monitoring

F.E-mail Archiving, Back-up andRetention

Policies

General Rule: applicant → CIO → Administrator

- A. Division or Non-Personnel Account
- B. Personnel Account
- C. Mailing Lists

Policies

D. E-mail Naming Convention

component@agency.gov.ph

division@agency.gov.ph

juan.delacruz@agency.gov.ph

juans.delacruz@agency.gov.ph

jsantos.delacruz@agency.gov.ph

js.delacruz@agency.gov.ph

Policies

E. Acceptable Use of the GovMail Service

- o Used in performance of official duties.

- o Code of Conduct and Ethical Standards for Public Officials and Employees (R.A. 6713).

- o Individual agency communication policies.

- o E-mail etiquette.

Policies

F. Prohibited Use of the GovMail Service

- o E-mail sent through GovMail Service for purposes outside of the performance of official duties and responsibilities.
- o Accessing, copying or deleting the e-mail of another Account Holder without the consent of the latter.
- o Account Holders shall not disclose their passwords to other persons, unless the Agency requires it.
- o Disruptive or offensive to other persons
- o Personal or commercial purposes or other

Policies

F. Prohibited Use of the GovMail Service

- Sending of **bulk mail** shall be prohibited unless such bulk mail is formally solicited.
- Memorandum Circular No. 78, entitled “Security of **Classified Matter** in Government Departments and Instrumentalities,” and amended by Memorandum Circular 196, shall not be sent using e-mail until specific guidelines are issued by the National Security Council, Department of Defense or the Office of the President for e-mail messages.
- Use of materials, procedures, devices or technologies that will enable **unauthorized access** to the GovMail Service is prohibited.

Policies

G. Privacy and Monitoring

- o Contents of the GovMailService are considered confidential government communication.
- o HTTPS, IMAP and PKI digital certificates shall be used to encrypt or secure the connection.
- o Digital certificates shall be used in authenticating users and the e-mail messages.

Roles and Responsibilities

- A. Information and Communication Technology Office
- B. Agency Personnel Head
- C. Agency Chief Information Officer
- D. E-Mail Account Administrator
- E. Authorized Users

Roles and Responsibilities

A. Information and Communication Technology Office

1. Communicate the policy.
2. Establish naming convention.
3. Maintenance and technical support.
4. Updates, patches, bugfixes.
5. Orient personnel head/administrator/CIO.
6. Provide admin and account management support.
7. Monitor legal agreements related to the service.
8. Communicate administrative matters to agency CIO.
9. Regulate and investigate matters relating to spam/counterfeit email.
10. Issue other policy documents as necessary.

Roles and Responsibilities

B. Agency Personnel Head

1. Ensure that GovMail is provided to employees.
2. Posting in accordance with RA9485.
3. Compliance with the naming convention.
4. Store and reproduce relevant information on account holders, as necessary
5. Training
6. Reporting in case of termination or suspension.
7. Compliance by account holder to the terms and conditions.

Roles and Responsibilities

C. Agency Chief Information Officer

1. Confirm/reject requests for account creation.
2. Direct administrator to create/suspend/terminate accounts.

Roles and Responsibilities

D. E-Mail Account Administrator

1. Assistance to users.
2. Act on spam.
3. Administer documentation on the use of GovMail.
4. Verify that email names comply with email naming.
5. Create/suspend/terminate as may be directed by CIO.
6. Establish tech support team.
7. Administer procedures in creation/suspension/termination of GovMailaccounts.
8. Tech support
9. Establish support team.
10. Inform and update personnel head of temporary unavailability.
11. Ensure email is read and acted upon.
12. Sign NDA covering the GovMail.

Roles and Responsibilities

D. E-Mail Account Administrator

1. Develop and implement GovMail service operations manual.
2. Implement email service policy.
3. Monitor and maintain service availability.
4. Conduct routine backup.
5. Period tests of the DRP.
6. Update email facility software.
7. Submit usage stats and compliance monitoring every month to the agency head.
8. Deactivate and archive email of users who have resigned/retired/separated or were suspended.
9. Ensure proper usage.
10. Sign the employee clearance form.

Roles and Responsibilities

E. Authorized Users

1. Sign the Authorized User Acknowledgement Form.
 2. Accountability for emails emanating from their accounts.
 3. Report violations to their supervisor.
 4. Read and comply with the service policy.
 5. Provide correct information regarding the creation of the GovMail account.
 6. Use GovMail for communications purposes.
 7. Keep password secure.
 8. Adhere to the naming convention.
- Report SPAM or counterfeit email.