GOVERNMENT OF ANDHRA PRADESH
ABSTRACT

ITE&C Department – "Email Policy of Government of Andhra Pradesh" - Orders – Issued.

INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS (INFRA) DEPARTMENT

G.O.MS.No. 15 Dated: 29.07.2015
Read the following

1. "E-mail policy of Government of India", notified in Gazette of India, Extraordinary No. 44, dated 18.02.2015.

2. "Policy on use of IT Resources of Government of India", notified in the Gazette of India Extraordinary No. 44, dated 18.02.2015.

ORDER:

1 Introduction

1.1 The Government uses e-mail as a major mode of communication. Communications include Government of Andhra Pradesh (GoAP) data that travel as part of mail transactions between users [1] located both within the country and outside.

1.2 This policy of Government of Andhra Pradesh lays down the guidelines with respect to use of e-mail services. GoAP email policy has been prepared complying with the Government of India (GoI) email policy vide 1st read above, as per clause 2.2 of the GoI policy, notified in Gazette of India, Extraordinary No. 44, dated 18.02.2015.

1.3 The Implementing Agency (IA) [2] for the GoAP e-mail service shall be National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology, GoI.

2 Scope

2.1 Only the e-mail services provided by the Implementing Agency notified by GoAP shall be used for official communications by all the organizations. The e-mail services provided by other service providers shall not be used for any official communication.

2.2 This policy is applicable to all the employees of GoAP and employees of those State Government Bodies that use the e-mail services of GoAP and also those State Government Bodies that choose to adopt this policy in future. The directives contained in this policy must be followed by all of them with no exceptions.

2.3 E-mail can be used as part of the electronic file processing in GoAP.

3 Objective

3.1 The objective of this policy is to ensure secure access and usage of GoAP e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the GoAP e-mail service amounts to the user's agreement to be governed by this policy.

3.2 All services under e-mail are offered free of cost to all officials under Departments / Offices / Statutory Bodies / Autonomous bodies (henceforth referred to as "Organizations [3]" in the policy) of GoAP.

3.3 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

4 Rolesspecified for implementation of the Policy

The following roles are required in each organization using the GoAP e-mail service. The official identified for the task shall be responsible for the management of the entire user base configured under that respective domain.

a. Competent Authority[4] as identified by each organization
b. Designated nodal officer[5] as identified by each organization
c. Implementing Agency (IA), i.e. National Informatics Center.

5 Basic requirementsof GoAP e-mail Service

5.1 **Security**

5.1.1 Considering the security concerns with regard toa sensitive deployment like e-mail, apart from the service provided by the IA, there would not be any other e-mail service under GoAP.

5.1.2 All organizations shall initiate the process of migrating their e-mail services to the centralized deployment of the IA, in case they are running their independent e-mail setup. For this purpose, the IA shall prepare and communicate a calendar to all Organizations.

5.1.3 For the purpose of continuity, the e-mail address of the organization migrating their service to the IA deployment shall beretained as part of the migration process. Wherever it is technically feasible, data migration shall also be done from the e-mail service of the organization to the e-Mail service provided by the IA.

5.1.4 From the perspective of security, the following shall be adhered to by all users of GoAP e-mail service:

a. There are certain security related risks inherent in e-mail communications which necessitate the adoption of requisite precautionary measures. Use of Digital Signature Certificate (DSC)[6] and encryption shall ,therefore, be mandatory for sending e-mails deemed as classified and sensitive, in accordance with the "AP Information Security Policy and Guidelines" to be notified by the GoAP.

b. It is strongly recommended that GoAPofficials on tour abroad should only use static IP addresses/Virtual Private Networks (VPN)[7]/One Time Password (OTP)[8] for accessing GoAP e-mail services. This is imperative in view of the security concerns that exist in other countries. OTP shall be delivered using easy to access channels like SMS.

c. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security to be sent by the IA. Updation of personal e-mail id(preferably from a service provider within India), in addition to the mobile number,shall also be mandatory in order to reach the user through an alternate means for sending alerts.

d. Users shall not download e-mails from their official e-mail account, configured on the GoAP mail server, by configuring POP [9] or IMAP[10] on any other e-mail service provider. This implies that users should not provide their GoAP e-mail account details (id and password) to their accounts on private e-mail service providers.

e. Any e-mail addressed to a user, whose account has been deactivated/deleted, shall not be redirected to anothere-mail address. Such e-mails may contain contents that belong to the government and hence no e-mails shall be redirected.

f. Users must ensure that their access devices (desktop/laptop/handheld, etc) have the latest operating system, anti-virus and application patches.

g. In case a compromise of an e-mail id is detected by the IA, an SMS alert shall be sent to the user on the registered mobile number. In case an "attempt" to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise), the IA reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer of that respective organization. In case of a situation when a compromise of a user id impacts the e-mail service or data security, the IA shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and nodal officer subsequently (over phone/SMS). SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

h. Forwarding of e-mail from the e-mail id provided by GoI to the government official's personal id outside the GoI e-mail service is not allowed due to security reasons. Official e-mail id provided by the IA can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

i. Auto-save of password in the government e-mail service shall not be permitted due to security reasons.

5.2 E-mail Account Management

a. Based on the user's request, IA will create two ids, one based on the designation and the other based on the name.

b. Government officers who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the e-mail account assigned in their personal namefor their entire life. However, the user would be given a new e-mail address by the IA. For continuity, the e-mail address "userid@ap.gov.in" would be retained for a period of one year, post resignation or superannuation.

5.3 Delegated Admin Console

Organizations can avail the "Delegated Admin Console" service from IA. Using the console the authorized person of an organization can create/delete/change the password of user ids under that respective domain as and when required without routing the request through IA. Organizations that do not opt for the admin console need to forward their requests with complete details to the IA's support cell (email.support@ap.gov.in).

5.4 **E-mail Domain & Virtual Hosting**

a. GoAP provides virtual domain hosting for e-mail. If an organization so desires, the IA can offer a domain of e-mail addresses as required by them. This implies that if an organization requires an address resembling the website that they are operating, IA can provide the same.

b. By default, the address "userid@ap.gov.in" shall be assigned to the users.

c. Organizations desirous of an e-mail address belonging to otherdomains (e.g.xxxx@police.ap.gov.in, yyyy@tourism.ap.gov.in) need to forward their requests to the IA.

5.5 **Use of Secure Passwords**

All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password policy are available in "Password Policy"at http://www.apit.gov.in/emailpolicy/guidelines.

5.6 **Privacy**

Users should ensure that e-mails are kept confidential. IAshall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

6 Responsibilities of User Organizations

6.1 **Policy Compliance**

a. All user organizations shall implement appropriate controls to ensure compliance with the e-mail policy by their users. IA shall give the requisite support in this regard.

b. The user organizations shall ensure that official e-mail accounts of all its users are created only on the e-mail server of the IA**.**

c. Nodal officer of the user organization shall ensure resolution of all incidents related to the security aspects of the e-mail policy. IA shall give the requisite support in this regard.

d. Competent Authority of the user organization shall ensure that training and awareness programs on e-mail security are organized at regular intervals. Implementing Agency shall provide the required support.

6.2 **Policy Dissemination**

a. Competent Authority of the concerned organization should ensure dissemination of the e-mail policy.

b. Competent Authority should use Newsletters, banners, bulletin boards etc, to facilitate increased awareness on the e-mail policy.

c. Orientation programs for new recruits shall include a session on the e-mail policy.

7 Responsibilities of Users

7.1 **AppropriateUse of E-mail Service**

a. E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name based ids can be used for both official and personal communication.

b. Examples of inappropriate use of the e-mail service

i. Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

ii. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

iii. Unauthorized access of the services. This includesthe distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

iv. Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

v. Creation and exchange of information in violation of any laws, including copyright laws.

vi. Wilful transmission of an e-mail containing a computer virus.

vii. Misrepresentation of the identity of the sender of an e-mail.

viii. Use or attempt to use the accounts of others without their permission.

ix. Transmission of e-mails involving language derogatory to religion, caste, ethnicity,sending personal e-mails to a broadcast list, exchange

of e-mails containing anti-national messages, sending e-mails with obscene material, etc.

x. Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation[11] of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

7.2 User's Role

a. The User is responsible for any data/e-mail that is transmitted using the GoIe-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b. Sharing of passwords is prohibited.

c. The user's responsibility shall extend to the following:

i. Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.

ii. The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii. Back up of important files shall be taken by the user at regular intervals. The IA shall not restore the data lost due to user's actions.

7.3 Use of IT Resources

All the users shall comply with "Policy on use of IT Resources of Government of India" in usage of IT Resources, notified vide 2nd read above,in the Gazette of India Extraordinary No. 44, dated 18.02.2015.

8 Service Level Agreement

The IA shall provide the e-mail services based on the Service Level Agreement (SLA) available at http://www.apit.gov.in/emailpolicy/guidelines.

9 Scrutiny of e-mails/Release of logs

9.1 Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies by the IA would be done only as per the IT Act 2000 and other applicable laws.

9.2 The IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny of e-mails or release of logs.

9.3 IA will maintain logs for a period of two years.

10 Security Incident Management Process

10.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of government data. Security incidents can be due to factors like malware, phishing [12], loss of a device, compromise of an e-mail id etc.

10.2 It shall be within the right of the IA to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

10.3 Any security incident, noticed or identified by a user must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.

11 Intellectual Property

Material accessible through the IA's e-mail service and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the government service and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

12 Enforcement

12.1 This "E-mail policy of GoAP" is applicable to all Government employees as specified in clause 2.2.

12.2 Each organization shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the organizations in this regard.

13 Deactivation

13.1 In case of threat to the security of the Government service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IA.

13.2 Subsequent to deactivation, the concerned user and the competent authority of that respective organization shall be informed.

14 Review

This policy shall be reviewed as deemed necessary, taking into account any change in the IT environment. The review shall take into consideration the following:

14.1 Impact on the risk profile due to, but not limited to, the changes in the deployed technology/e-mail architecture, regulatory and /or legal requirements.

14.2 The effectiveness of the security controls specified in the policy.

14.3 Advancement in the technologies underlying the e-mail services.

(BY ORDER AND IN THE NAME OF THE GOVERNOR OF ANDHRA PRADESH)

B.SREEDHAR
SECRETARY TO GOVERNMENT

To
All the Departments of Secretariat
All the District Collectors & Magistrates, AP
All the HoDs
The SIO, National Informatics Centre, A.P. Unit

Copy to:
The Chief Minister's Office/Chief PRO to C.M.
The OSD to Hon'ble Minister for Information Technology, Andhra Pradesh
The PS to PFS, Andhra Pradesh
The PS to OSD to Hon'ble CM, Andhra Pradesh
The PS to Chief Secretary to Government of Andhra Pradesh
The PS to Advisor, ITE&C, Andhra Pradesh

//FORWARDED BY ORDER//

SECTION OFFICER

GLOSSARY

(G.O.MS.No. 15, date : 29.07.2015 of ITE&C Det., GoAP)

S.No	TERM	DEFINITION
1	**Users**	Refers to officers/personnel who are accessing the government services.
2	**Implementing Agency (IA)**	For the purpose of this policy, the agency to be notified by the GoAP.
3	**Organization**	For the purpose of this policy, organization refers to all departments/offices/statutory bodies/autonomous bodies, of GoAP.
4	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his organization
5	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the organization
6	**DSC**	A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the e-mail was created by a known sender, such that the sender cannot deny having sent the e-mail (authentication and non-repudiation) and that the e-mail was not altered in transit (integrity).
7	**VPN**	A **virtual private network** extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network
8	**OTP**	A **one-time password** (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords
9	**POP**	**POP i**s short for **P***ost* **O***ffice* **P***rotocol,* a protocol used to retrieve e-mail from a mail server.
10	**IMAP**	IMAP is short for "The Internet Message Access Protocol", a protocol used to retrieve e-mail from a remote mail server. Unlike POP, in IMAP, Messages are displayed on your local computer but are kept and stored on the mail server. IMAP allows you to sync your folders with the e-mail server which is not possible using POP.
11	**Deactivation**	**Deactivation** of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account shall bounce to the sender
12	**Phishing**	**Phishing** is a fraudulent attempt, usually made through e-mail, to steal a user's personal information. Phishing e-mails almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate organisations would never request this information via e-mail. Users should never click on a link. A user should always type a URL in the browser even if the link appears genuine**.**

SECRETARY TO GOVERNMENT