F. No. 2(22)/2013-EG-II
Ministry of Communication & Information Technology
Department of Electronics & Information Technology

Guidelines for E-mail Account Management and Effective E-mail Usage

October 2014
Version 1.0

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi – 110003

Table of Contents

1. Introduction:

1.1 Government of India has formulated the **"E-mail Policy of Government of India"**. This document supports the implementation of this policy by providing necessary guidelines regarding "**E-mail Account Management and Best Practices for Effective E-mail Usage".**

2. E-mail Account Management

2.1 Creation of E-mail Addresses

Based on the request of the respective organizations, IA will create two ids, one based on the designation and the other based on the name. Designation based id's are recommended for officers dealing with the public. For ids created based on designation, it is strongly recommended that One Time password (OTP)[3] is used for authentication. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the competent authority.

a) In addition to the government users as mentioned in the "E-mail Policy" of Government of India , accounts for outsourced/contractual[4] employees shall also be created after due authorization from the competent authority of that respective organization[5]. These accounts shall be created with a pre-defined expiry date and shall be governed by the "E-mail Policy of Government of India".

b) Account can be created by the authorized person from an organization by using the "Delegated Admin Console" or by routing their request to IA. For more details refer to the "E-mail Policy of Government of India".

2.2. Process of Account Creation

a) An e-mail account has to be created for every user in an organization. The user needs to request for an account by filling the form available on the e-mail site and send it to the nodal officer of respective organisation.

b) The nodal officer of an organization shall authorize creation of new e-mail accounts.

c) The e-mail account is created based on the NIC e-mail addressing policy available at http://www.deity.gov.in/content/policiesguidelines/ under the caption "E-mail Policy".

d) If a user organization wants to adopt an addressing policy that represents their identity, the IA would need to be informed by the user organization. However "id" uniqueness needs to be maintained. Hence prior to sending a request for "id" creation, nodal officer should use the "idlookup" tool available on the IA's e-mail site to ensure "id" availability.

2.3 Process of Handover of Designation Based E-mail Ids

a) Users shall hand over the designation based id to their successor prior to moving out of the office. User can continue to use the name based id assigned to them on the Government e-mail service during their entire tenure in GoI.

b) Prior to leaving an organization on transfer, the user to whom the designation based id had been assigned shall ensure that the password for the id is changed. The successor shall need to get the password reset after taking over the post.

c) The nodal officer in each organization shall ensure that the password is changed prior to giving "No-Dues" to the user.

d) The above process shall be followed without any exception. If an id is misused, the respective nodal officer of each organization shall be held accountable.

e) The nodal officer and the user shall inform the IA prior to their superannuation/transfer of the user by sending an e-mail to support@gov.in

2.4 Data Retention

a) Users are responsible for e-mails saved in their folders as they deem appropriate for e.g. Inbox, Sent Mail, any other folder created by the user. E-mails shall be automatically purged from 'Trash" and "Probably Spam [6]" folders after a specified time period by the IA.

2.5 Data Backup

a) The IA takes a backup of the e-mail data on a regular basis to ensure timely recovery from a system failure/crash/loss impacting the service.

b) Each user is responsible for the individual e-mails stored in their folders. The IA shall not be responsible for any accidental deletion of e-mails by the user.

c) E-mails lost as a result of wrong configuration of the local mail clients (e.g. Outlook/Eudora/Thunderbird, etc) shall not be the responsibility of the IA.

d) The IA shall not offer a service for restoration of lost data due to an action committed by the user.

e) In the eventuality of a disaster/calamity, all possible attempts to restore services and content shall be made. However, in circumstances beyond the control of the IA, it would not be held responsible for loss of data and services.

2.6 Deactivation of Accounts:

2.6.1 Deactivation [7] or deletion of an account shall occur under the following conditions:

a) **The officer retires/resigns from Service**: The user shall surrender their official designation based account prior to getting relieved from the service. However, name based e-mail addresses can be retained as per the conditions specified in clause 2.8 below. It is mandatory for the users to inform the IA regarding their superannuation/resignation by sending a mail to support@gov.in

b) **The officer is no longer in a position to perform his duties** (death/missing, etc).The name based e-mail id of the user shall be deleted by the IA. The nodal officer of that respective organisation shall inform the IA by sending a mail to support@gov.in

c) **Inactive account**: Any account which is inactive for a period of 90 days shall be deactivated under intimation to the concerned department. The user id along with the data shall be deleted from the e-mail system after a period of 180 days, if no request for activation is received during this period. Subsequently, all formalities shall need to be completed for re-opening of the said account with the same id, subject to availability. In such cases, data from the backup shall not be restored.

d) **Violation of policy**: The authorized person at the organization under whose request the account has been created shall inform the IA when any of the above conditions are triggered. Intimation shall be sent to support@gov.in

e) **Misuse of account**: Whenever information is not sent

or sent at a later date, the IA shall not be responsible in case the account is misused and comes under the scrutiny of the designated investigating agencies.

2.6.2 Based on the conditions above, and as per the status of the officer, competent authority of respective organizations shall introduce a process to ensure that e-mail id is either deactivated/deleted/password changed, prior to giving "no-dues" to a user

2.7 Desktop Protection

a) Spam filters and anti-virus filters have been configured at the e-mail gateways by the IA. These filters are there to protect the e-mail setup from viruses and unsolicited e-mail. Whilst these filters are constantly updated, the IA cannot guarantee that it shall provide 100% protection against all viruses and spam.

b) Users using the desktop/laptop/handheld devices shall ensure that all recommended best practices are followed from time to time.

2.8 Status of account in case of Resignation or Superannuation

a) At the time of resignation or superannuation, users shall inform the nodal officer/IA regarding their resignation or superannuation through the competent authority.

b) The nodal officer/IA shall accordingly change the user's account status. This shall be made mandatory before the concerned organisation gives a "No-Dues" certificate to the user and the retirement benefits are processed.

c) The designation based id shall be processed as mentioned against clause no 2.3 above.

d) As mentioned in the "E-mail Policy of Government of India",

a user who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the e-mail address userid@gov.in for one year post resignation or superannuation. Subsequently, a new e-mail address with the same user id but with a different domain address (for instance, userid@pension.gov.in), would be provided by the IA for their entire life. It is expected that within one year, users shall change the e-mail address at all places as required by them. During this one year, if the name based account is not used for a period of 90 days, the account shall be deleted and no request for activation shall be accepted by the IA.

e) The use of the account post retirement shall be governed by the current policy and subsequent updates of the same.

f) Availability of a government e-mail id post retirement does not entail an employee to any remuneration.

g) In case a user resigns from service before completion of 20 years, the name based e-mail id shall be deleted as part of the "No-Dues" process. These needs to be ensured by the competent authority of each organization and the IA accordingly shall be informed.

3. Secure access of GoI E-mail services for Officials stationed outside India/ working in Sensitive Offices.

3.1 Officials shall be issued the VPN token after completing the registration process as indicated on the IA's VPN services site (http://vpn.nic.in). For any queries/troubleshooting, mail can be sent to vpnsupport@gov.in. OTP shall be delivered using easy to access channels like mobile agents/SMS/alternate e-mail address (preferably from a service provider within India)/hard and soft tokens. NIC shall issue the OTP token based on user's request and preferred mode of access.

3.2 Prior to integration of VPN and OTP with the e-mail services, a pilot will be conducted with select missions abroad and changes in the deployment will be introduced based on challenges encountered, if any.

4. Recommended Best Practices

Users are advised to adopt the following best practices for safe usage of e-mail services.

a) All users must check their last login details while accessing their e-mail accounts by using the application created for this purpose. More details are available in the "NIC Services and Usage Policy" available at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy". This application helps in making users aware of any unauthorized access to their account.

b) Use of encryption and DSC [8] is mandatory for sending any mail deemed as classified or sensitive.

c) It is strongly recommended for users working in sensitive offices to use OTP for secure authentication.

d) The user should change passwords on a periodic basis or as per the password policy available at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

e) It is recommended that the users should logout from their mail accounts whenever they leave the computer unattended for a considerable period of time. The current e-mail application of the IA has an auto-logout feature that is triggered after a pre-defined period of inactivity.

f) Other than Government websites, the e-mail ids and e-mail address assigned on the Government e-mail service should not be used to subscribe to any service on any website. Mails received from sites outside the Government may contain viruses, Trojans, worms or other unsafe contents.

g) It is strongly recommended that the users use the latest version of their Internet browser for safe browsing.

h) The "save password" and auto complete features of the browser should be disabled.

i) The files downloaded from the Internet or accessed from the portable storage media should be scanned for malicious contents before use.

j) To ensure integrity of the downloaded files, digital signatures/hash values should be verified wherever possible.

k) Before accepting an SSL [9] certificate, the user should verify the authenticity of the certificate. User should type the complete URL [10] for accessing the e-mails rather than click on a mail link for access. This is recommended to avoid phishing [11] attacks.

l) The IA does not ask for details like login id and password over e-mail. Users should disregard any e-mail that requests for the same, and should refrain from sharing such details over e-mail with anyone.

m) Sending an e-mail with an infected attachment is the most common means adopted by a hacker to send malicious content. Hence, it is mandatory to install and maintain latest operating system, anti-virus and application patches to prevent infection.

n) All attachments must be scanned with an anti virus program before they are downloaded/executed, even if such e-mails are received from a familiar source.

o) User should exercise caution while forwarding mails as they may contain malware. User should ensure authenticity of the source and safe nature of the attachments before forwarding any mail.

p) E-mails identified as spam are delivered in the "Probably Spam" folder that exists in the user's mailbox. Hence it is recommended that the users should check the "Probably Spam" folder on a daily

basis.

q) Attachments should be opened only when the user is sure of the nature of the e-mail. If any doubt exists, the user should contact the sender to verify the authenticity of the e-mail and/or the attachment.

r) User should use due discretion while creating classified and sensitive documents. Unless required otherwise, the documents should be created in manner that it cannot be edited.

s) Users should not open e-mails from dubious sources.

t) User should exercise caution in opening mails where links are embedded in the mail. The authenticity and the safe nature of the link should be ascertained before clicking the link.

GLOSSARY

S.No	TERM	DEFINITION
1.	**Implementing agency (IA)**	For the purpose of E-mail policy, the implementing agency is "National Informatics Centre"
2.	**User**	Refers to Government/State/UT employees/contractual employees who are accessing the Government services
3	**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
4	**Outsourced/contractual employees**	An employee who works under contract for GoI. A contract employee is hired for a specific job or assignment. A contract employee does not become a regular addition to the GoI staff and is not considered a permanent employee of GoI
5	**Organization**	For the purpose of this policy, organisation refers to all ministries/departments/offices/statutory bodies/autonomous bodies, both at the central and state level. Government organizations offering commercial services are not included
6	**SPAM**	**Spam** is the use of e-mail systems to send unsolicited bulk e-mails, especially advertising, indiscriminately.
7	**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
8	**DSC**	A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a 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).

9	**SSL**	The **Secure Socket Layer (SSL)** is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet.
10	**URL**	**URL** stands for **Uniform Resource Locator**. A URL is a formatted text string used by Web browsers, e-mail clients and other software to identify a network resource on the Internet. Network resources are files that can be plain Web pages, other text documents, graphics, or programs.
11	**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**.**