

F. No: CEPT / IT Policies / 2015
Government of India
Ministry of Communications & IT
Department of Posts
(Center for Excellence in Postal Technology)

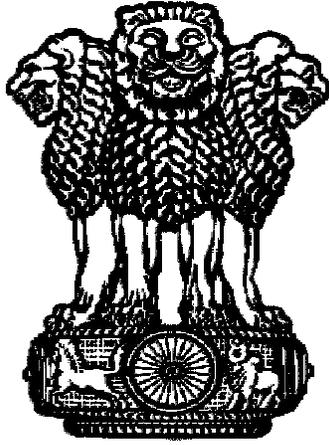
CEPT, Mysore - 570010
Dated: 06-11-2015

Subject: Email Policy of Department of Posts.

The competent authority has approved the Email Policy of Department of Posts (version 1.0) along with its annexures which is published for information and compliance by all the email users of DoP.



[K Balasubramanian]
General Manager, CEPT



सत्यमेव जयते

**E-mail Policy Of
Department of Posts**

October 2015

Version 1.0

**Department of Posts
Ministry of Communications & Information Technology
Government of India
New Delhi - 110001**

Table of Contents

1.	Introduction	3
2.	Scope	3
3.	Objective	3
4.	Roles specified for implementation of the Policy	4
5.	Basic requirements of DoP e-mail Service	4
6.	Responsibilities of DoP	6
7.	Responsibilities of Users	7
8.	Service Level Agreement	9
9.	Scrutiny of e-mails / Release of logs	9
10.	Security Incident Management Process	10
11.	Intellectual Property	10
12.	Enforcement	10
13.	Exception Management	11
14.	Audit of E-mail Services	11
15.	Review	11
	List of Annexures	12
	GLOSSARY	12

1. Introduction:

- 1.1** Email communication that includes data transmission between users,^[1] located both within the country and outside, is being widely used by the Department of Posts [DoP] as an official communication.
- 1.2** Through this document the DoP is laying down the "E-mail Policy"^[2] for "DoP e-mail Services"^[3]. The Implementing Agency (IA)^[4] for the DoP email service shall be CSI Vendor of India Post IT Modernization Project.

2. Scope:

- 2.1** All government employees working within the DoP shall use DoP email services for all the official communication apart from the written official communication. The use of e-mail service of other private service providers shall be strictly limited to unofficial/personal communication and shall not be used for any official communication.
- 2.2.** This email policy shall be applicable to all those employees of the Department of Posts who have been provided with an official email ID under India Post Domain i.e. email id ending with **@indiapost.gov.in** and those who use the email services of the department. The directives contained in this policy are to be followed by all such employees without any exception.

3. Objective:

- 3.1** The objective of this policy is to ensure secure access and usage of DoP e-mail services by its users^[1]. Users have the responsibility to use this resource in an efficient, effective, lawful and ethical manner. Use of the DoP 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 the employees of the DoP. More information about the DoP Email Services are annexed (Annexure -1) to this "Email Policy".
- 3.3** This policy supersedes any other email policy previously laid down by the DoP.

4. Roles specified for implementation of the Policy:

4.1 The following roles are specified in DoP with regard to email services. The individual identified for the task will be responsible for the management of the entire user base configured under the India Post domain.

4.1.1 Competent Authority^[5]: An officer nominated for this purpose by the Department of Posts.

4.1.2 Designated Nodal Officer^[6]: An officer nominated by the Competent Authority.

4.1.3 Controlling Officer^[7]: An officer who is immediate superior/reporting officer/disciplinary authority for the user.

4.1.4 Implementing Agency (IA)^[4]: IA for DoP email service is CSI Vendor of IT Modernization Project of DoP.

5. Basic requirements of DoP e-mail Service:

5.1 Security:

5.1.1 Considering the security concerns, there shall be single official email service of Department of Posts under India Post domain and all official communications should be exchanged through official email id only.

5.1.2 From security perspective, following shall be adhered to by all users of DoP e-mail service:

- i.** Relevant Policies framed by Ministry of Home Affairs, relating to classification, handling and security of information shall be followed.
- ii.** Use of 'Digital Signature Certificate (DSC)^[8] and 'E-mail Encryption^[9] shall be mandatory for sending e-mails deemed as classified and sensitive in accordance with relevant policies of Ministry of Home Affairs.
- iii.** Updation of current mobile numbers under the personal profile of users shall be mandatory for security reasons. The number shall be used for alerts and information regarding security. 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 as an alternate means for sending alerts.

- iv.** Users shall not download/forward/redirect e-mails from their official e-mail account, configured on the DoP mail server, to their personal email accounts outside DoP email servers.
- v.** Any e-mail addressed to a user, whose email account has been deactivated^[10], shall not be redirected to another e-mail address outside DoP email servers. Such e-mails may contain privileged information belonging to DoP and hence no such e-mails shall be redirected.
- vi.** Users shall ensure that the access device (Desktop/Laptop/Handset etc.) have the latest operating system, anti-virus and application patches.
- vii.** In case a 'compromise of an e-mail id'^[11] 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 email 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), then password of that particular e-mail id shall be reset. Consequently User will require to call the IA's Service Desk^[12] or use the "Forgot Password" option to set a new password.
- viii.** In case of a situation when a compromise of a user id impacts the e-mail service/the data security or an input is received from the authorized investigating agency regarding such a compromise, the password of the concerned user id shall be reset by the IA. This action shall be taken on an immediate basis and the information shall be provided to the user subsequently (over Phone/SMS/alternate email id).
- ix.** Official e-mail id provided by DoP 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.
- x.** The email ids of DoP email service must not be used to subscribe to any service or any website other than the GoI websites & services because non GoI websites may try to flood the inbox with mails which may contain viruses, Trojans, worms/other unsafe contents or spammers may try to send bulk SPAM.

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

5.2 E-mail Account Management:

5.2.1 Details pertaining to e-mail account management are annexed (Annexure -2) to this "Email Policy" which contains policy statements on creation of email accounts, process for email account creation, process of handover of functional email ids etc. along with 'Recommended Best Practices' for safe usages of email services.

5.3 Use of Secure Passwords:

5.3.1 All users accessing the DoP e-mail services must adhere to the "Password Policy" for setting a password to their email account which guarantees their mail account are more secured. More details about the Password Policy are annexed (Annexure -3) to this "E-mail Policy".

5.4 Privacy:

5.4.1 Users should ensure that official e-mails of the DoP are kept confidential. Users must also ensure that information regarding their password or any other personal information which may lead to the compromise of the email account is not shared with anyone.

5.4.2 All possible precautions shall be taken by IA on maintaining privacy of the user.

6. Responsibilities of DoP:

6.1 Policy Compliance:

6.1.1 Competent Authority shall implement appropriate controls to ensure compliance with the e-mail policy by the users of DoP email service. IA shall give the requisite support in this regard.

6.1.2 Nodal officer shall ensure resolution of all incidents related to the security aspects of the e-mail policy through IA.

6.1.3 The training wing of DoP 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:

- 6.2.1** Email Policy dissemination activity involves distribution of the policy and all its relevant documents to the respective users. Competent Authority should ensure dissemination of the e-mail policy.
- 6.2.2** The email policy should be made available to the users for viewing /download. Read only access should be given to the intended users.
- 6.2.3** Training and awareness programs on the email policy should be organized periodically.
- 6.2.4** Newsletters, banners, bulletin boards etc. should be used to facilitate increased awareness on the e-mail policy.
- 6.2.5** Employees' orientation programs should include a session on the e-mail policy.

7. Responsibilities of Users:

7.1 Appropriate Use of E-mail Service:

- 7.1.1** E-mail is provided as a professional resource to assist users in fulfilling their official duties. Thus the communications sent through email becomes a part of the official record of the office in which user is working. Communications emanating from the user, on behalf of the office should be sent using the functional email ids provided to the designation. Personal communications from the user may be sent using by name based email ids provided. This is to ensure that all official communications sent from the office are available to the next incumbent as office records. Similarly communications addressed to an office should be sent to the functional email ids only. If the sender desires to seek the personal attention of the recipient in view of the urgency/importance of the matter then a copy can be marked to the by name id of the recipient.
- 7.1.2** The email service should not be put to any use which is considered inappropriate or impinges on National Security or violates any policy of the Department of Posts and/or GoI. Examples of inappropriate uses are:
 - i.** Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening, using language derogatory to religion, caste, ethnicity, sex etc.
 - ii.** Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

- iii. Unauthorized access of the services. This includes, for example, the 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. Willful 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 email accounts of other users without their permission.
- ix. Transmission of e-mails containing anti- national messages/obscene materials.
- x. Sending personal emails to a broadcast list.
- xi. Use of 'Distribution Lists'^[13] for the purpose of sending e-mails that are personal in nature, such as personal functions etc.
- xii. Sending messages to harass or intimidate other.

7.1.3 Any case of inappropriate use of email accounts shall be considered as violation of the policy and may result in Deactivation of the email account besides attraction of disciplinary action against user as deemed appropriate. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

7.2 User's Role:

7.2.1 The User is responsible for any data/e-mail that is transmitted using his/her email account over the DoP e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the email account used for sending it.

7.2.2 Sharing of passwords is prohibited.

7.2.3 Each individual is responsible for his/her email account, including the safeguarding of access to the email account. An email originating from an account is deemed to be authorized by the email account owner. It is the responsibility of the email account owner to ensure compliance with DoP email Policy guidelines.

7.2.4 The user's responsibility shall extend to the following:

- i. Users shall be responsible for the activities carried out on their client systems/other systems, using the email 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.
- iv. If the designation based email id is delegated to any one (only) authorized official, proper record regarding such authorization may be kept on record along with the acknowledgement of the authorized official. In such cases the authorized official should comply with all terms and conditions of DOP email policy without fail while handling the delegated designation based email id.
- v. Users shall not delete any email conversation in their functional email ids provided to their designation once they get transfer orders or at the time of their retirement, to ensure that the institutional memory, in the form of emails in their functional email id is passed on to the next incumbent.

8. Service Level Agreement:

- 8.1** The IA shall provide the e-mail services to the DoP based on the "Service Level Agreement (SLA)" as per the contract.

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 and other organizations by the IA would be done, after due approval from the competent authority, only as per the IT Act 2000 and other applicable laws.
- 9.2** The Department of Posts will provide the necessary cooperation to such agencies when approached through authorized channel. The consent of the user in this regard shall not be taken.
- 9.3** 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.
- 9.4** IA will maintain logs for a period of two years.

10. Security Incident Management Process:

- 10.1** An incident response and management process is necessary for detecting security incidents, minimizing loss and damage, mitigating the weaknesses that were exploited and restoring information assets in a timely manner. This process is applicable to all policy violations reported by the IA or the Users.
- 10.2** A security incident is defined as any adverse event which occurs on any part of the email services and that can impact the availability, integrity, confidentiality and authority of Government data. Security incidents can be due to factors like compromise of a user account, spread of SPAM^[14]/Virus that affects the system & service. Detection of a Phishing^[15] site of the email service of DoP, Loss of a portable storage media containing government data, violation of policy thereby causing a security breach, other consequences affecting security of email services etc.
- 10.3** DoP through the IA reserves the right to deactivate/remove any feature of the Email service if it is deemed as a threat and can lead to a compromise of the service.
- 10.4** Any security incident, noticed or identified by a user must immediately be brought to the notice of the IA's Service Desk which in turn be reported to Indian Computer Emergency Response Team (CERT-In) by the competent authority if deemed fit/depending on the severity.

11. Intellectual Property:

- 11.1** Material accessible through the DoP 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" is applicable to all employees of DoP & those who uses the DoP email services as specified in clause 2.2.
- 12.2** It is mandatory for all users to adhere to the guidelines of this policy without exception. Violation of this Policy will amount to misconduct under CCS (Conduct) Rules.

12.3 DoP shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance in this regard.

13. Exception Management:

13.1 For any exception/deviation, the user shall take approval from the Competent Authority of DoP. The request will be processed through the Service Desk being operated by IA and will be executed only after approval from the Competent Authority of DoP.

14. Audit of E-mail Services:

14.1 The competent authority shall ensure that security audit of DoP email services is conducted periodically by an agency empaneled by the Government of India.

15. Review:

15.1 This Policy shall be reviewed at the time of any change in the IT environment or once every year, whichever is earlier. The review shall be carried out for assessing the following:

15.1.1 Impact on the risk profile due to, but not limited to, the changes in the deployed technology/network security architecture, regulatory and/or legal requirements.

15.1.2 The effectiveness of the security controls specified in this policy.

15.1.3 Other changes in the Policy, as deemed necessary.

15.2 This review shall be made by DoP Competent Authority in consultation with various stakeholders as deemed necessary. As a result of the review, the existing policy may be updated or modified.

= = = / = = =

List of Annexures

Annexure 1: DoP E-mail Services & Usages Policies V.1.0

Annexure 2: DoP E-mail Account Management Guidelines V.1.0

Annexure 3: DoP Password Policy V.1.0

GLOSSARY

SL	Term	Definition
1	Users	Refers to DoP employees and those who are accessing the DoP email services.
2	Email Policy	Refers to the Policy document that lays down the guidelines with respect to use of e-mail services.
3	DoP Email Services	Refers to the centralized email service being used by DoP as part of implementation of CSI component of India Post IT Modernization Project.
4	Implementing Agency (IA)	For the purpose of this policy, the implementing agency is CSI Vendor of IT Modernization Project of DoP.
5	Competent Authority	Officer responsible for taking and approving all decisions relating to DoP email services which will be nominated for this purpose by the Department of Posts.
6	Nodal Officer	Officer responsible for all matters relating to this policy who will coordinate on behalf of DoP. It will be nominated by Competent Authority.
7	Controlling Officer	Officer who is immediate superior/reporting officer/disciplinary authority for the user of DoP email services.
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). Digital signatures are commonly used for software distribution, financial transactions and in other cases where it is important to detect forgery or tampering.

9	Email Encryption	Email encryption is encryption (a process of encoding messaged or information in such a way that only authorized person can read it) of email messages to protect the content from being read by other entities than the intended recipients. Email encryption may also include authentication.
10	Deactivation	Deactivation of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account will bounce to the sender.
11	Compromise of an email account	<p>An user can be sure that his/her email account has been compromised if he/she experiences the following issues :</p> <ul style="list-style-type: none"> • Contacts has received suspicious messages for user's account; • Contacts and/or mails have gone missing; • A warning about suspicious activity has been received from Last Account Activity; etc.
12	IA's Service Desk	Refers to the support desk being operated by the Core System Integrator (CSI) of India Post IT Modernization Project. Users can register any service request or report any incident/complaint to the CSI Service Desk.
13	Distribution List	Refers to a list of more than one email ids grouped for convenience in sending mails. Using distribution list a user can send a particular mail to more than one email ids using the list name. Mail will be sent to all the email ids listed under a particular distribution list.
14	SPAM	SPAM is the use of email system to send unsolicited bulk e-mails, especially advertising, indiscriminately.
15	Phishing	<p>Phishing is a fraudulent attempt, usually made through e-mail, to steal a user's personal information.</p> <p>The best way to prevent a phishing attack is to learn how to recognize a phish. Phishing e-mails usually appear to come from a well-known organization and ask for a user's personal information – such as credit card number, social security number, bank account number or password. In order for internet criminals to successfully "Phish" a user's personal information, they must get a user to go from an e-mail to a website.</p> <p>Phishing e-mails will almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate organizations 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.</p>

END OF DOCUMENT

DoP Email Services & Usage Policies V.1.0

Department of Posts (DoP) provides a range of services under “DoP email services” to its users.

Key services offered are:

1. **E-mail Services:** DoP provides the E-mail services to its users to send and receive emails from anywhere in the internet space and / or within DoP Intranet.
 - 1.1 However Users shall note that the size of the Mail Box over DoP Mail Server is limited to 100 MB only and hence users, in order to manage the mail exchanges within the allocated size, shall configure Outlook Client (available along with MS Office Suite) to their mail box. Users shall ensure that all mail exchanges is available in the respective Outlook Data file.
 - 1.2 User shall also ensure that periodical backup of the Outlook Data file is taken and kept in a secured manner to avoid loss of email messages in the event of any unforeseen irreparable damage to the Desktop/laptop in which the mail box is configured to Outlook Client. In such circumstances the email messages can be restored from the backed up Outlook Data file. Users are recommended to take weekly backup of the Outlook Data file.
2. **Instant Messaging:** DoP provides the Instant Messaging services to its users coupled with the email service. User of DoP email services will be able to send instant messages to a single individual user or to a group of users. Users will also be able to send and receive files from within IM conversations.
3. **Business Continuity as a service:** Email service is an extremely critical service; and hence it is mandatory to ensure service continuity under all circumstances. In order to ensure that the service is available under all conditions, in addition to the primary site, a secondary site i.e. a Disaster Recovery (DR) site has been configured for the email services. The entire data is replicated to the DR site. In the eventuality of a service failure at the primary site, the services roll over to the DR site thereby giving users uninterrupted access.

4. **Mail Gateway Service:** Gateway services offered by DoP through CSI vendor ensures that any mail traffic, whether inbound or outbound from DoP Mail Servers, shall be scanned by the DoP SMTP gateways for scrubbing for any possible SPAM, Malwares, Trojans & Viruses. This is extremely necessary as scanning of traffic ensures that infections do not reach the DoP network. This also enables DoP for content management of the messages being exchanged.
5. **Email Distribution List Services:** This service is offered using the concept of Distribution Lists (DLs). A DL enables an user to send mails to all email ids which are members of the DL using the DL email id instead of individual email ids. Users of DoP email services may avail this service to create customized distribution lists based on their requirements. This service allows the end user to manage their own customized DLs locally at their account level. Additionally standard server level DLs viz. All CPMG, All PMG, All DPS etc. has also been created and rights to use these DLs are being allowed on need basis after request from the user concerned. Users may send mails for rights to use a particular server level DL to IA's Service Desk.
6. **Secure Authentication:** For the purpose of secure authentication, users of DoP email services may use Digital Signature Certificate (DSC).
7. **Mail Encryption:** Mail encryption is enabled by default in the exchange process between sender and recipient of mail. Users can, as an added security, use the DSC as well.
8. **Last Login Service:** As security is a prime concern in today's cyberspace, IA will provide the Last login service. This service allows a user to check the login details of his/her email id for last 30 days. The details include IP Address, Date, Time and Location of access. The console shows access using all protocols i.e. IMAP / POP and Web.
9. **Forgot Password:** In order to empower a user to reset his / her password, IA will provide the "Forgot password" service. This service allows a user to reset the password without the intervention of IA's Support / Service Desk.
10. **Calendar Service:** This service enables users to record events and tasks, share calendar with others, view others' calendars, invite other calendar users to events and set reminders and notifications for an event.
11. **SMS and Email notification alerts:** IA will send the following notifications:

11.1 SMS Alerts: In case a password compromise of an user id is detected, a SMS alerts will be send on the registered mobile number of the user. This is done, as security regarding a critical service like Messaging is extremely important. If a user does not follow the instructions given in the SMS even after 5 alerts the password shall be reset by the IA. The user will need to call the IA's Service Desk to get a new password or use the "Forgot Password" option to set a new password.

11.2 Email alerts: In case 3 failed login attempts are detected for an user id an email will be sent containing the IP details, Location and Time Stamp of the failed attempts. This mail is to be sent to alert the user as these attempts may be efforts by unauthorized person to compromise the password.

== = / = ==

Table of Contents

1.	Introduction	3
2.	Email Accounts Management	3
	2.1 Creation of Email Addresses	3
	2.2 Process of Account Creation	3
	2.3 Process of Handover of Functional Email Ids	5
	2.4 Data Retention	5
	2.5 Data Backup	6
	2.6 Desktop Protection	6
	2.7 Deactivation of Accounts	7
	2.8 Status of Account in case of Resignation or Superannuation	8
3.	Recommended Best Practices	9
	Annexure 2A _ Email Account Creation Form	11
	GLOSSARY	14

1. Introduction:

- 1.1** Department of Posts (DoP) has formulated the **“E-mail Policy of Department of Posts”**. This document supports the implementation of this policy by providing necessary guidelines regarding **“E-mail Account Management and Best Practices for Effective E-mail Usages”**.

2. E-mail Account Management:

2.1 Creation of E-mail Addresses:

- 2.1.1** Email IDs (Name Based) will be created for all employees of DoP under Group 'A' & Group 'B' (Gazetted) and Inspector Posts category.
- 2.1.2** For other categories of employees the name based email IDs will be created on need basis.
- 2.1.3** Functional Email Ids (Designation Based) shall be created for all the standard designations available in the department. Other functional email ids shall also be created on need basis.
- 2.1.4** Email accounts shall also be created for all the functional units like Post Offices and RMS Offices.
- 2.1.5** Accounts for “Outsourced / Contractual Employees”^[1] shall also be created after due authorization from the competent authority. These accounts will be created with a predefined expiry date and shall be governed by the “Email Policy of Department of Posts”.

2.2 Process of Account Creation:

- 2.2.1** An e-mail account will be created upon user request by filling out the prescribed “Email Account Creation Form” (Annexure 2A) and sending it to the Nodal Officer. The details of Nodal Officer & manner of submission of form will be furnished on the email website and on the said form. The Nodal Officer shall authorize creation of new e-mail accounts.

2.2.2 Forms should be complete in all respects for the account to be created. After authorization, Nodal Officer will send this form to IA for creation of email account.

2.2.3 Upon creation of the email account, the IA will store the documents in a secured manner as per the workflow notified.

2.2.4 Time taken to create a single account by IA is one working day. For bulk creation of accounts (up to 20) IA will take a maximum of 2 working days and if the list of accounts to be created exceeds 100, IA can take up to a maximum of 5 working days to create all the accounts.

2.2.5 The email account is created based on "E-mail Addressing Policy of Department of Posts" given below :

2.2.5.1 Name Based email IDs will be created with their first name and last name separated by a dot (.) for example, firstname.lastname@indiapost.gov.in. Email will not contain the middle name of the employee. However the Display Name of the email Id will be the complete name of the employee.

2.2.5.2 In case, more than one Group A / Group B employee exists with same name, numerals will be put after the first name, for example, firstname1.lastname@indiapost.gov.in.

2.2.5.3 If the name of a Group A / Group B employee consists of only one word, i.e. without last name then the email id created will be name@indiapost.gov.in.

2.2.5.4 Employees who already have by name email IDs (migrated from NIC servers to DoP servers) have the option to retain the existing email ID or switch over to new email Id as per the new naming policy.

2.2.5.5 The various categories of functional email ids (e.g. Designation based, Office based, specific purpose based etc.) will be created with easy to understand nomenclature and Display Name.

2.3 Process of Handover of Functional E-mail Ids:

- 2.3.1** The Functional E-mail Id (Designation Based, Office Based, Unit based, Specific Purpose etc.) should be handed over by the user to their successor prior to moving out of the office. The word "handover" implies that the user will supply not only the 'email login credentials' but also the latest backed up 'outlook data file' in restorable condition, wherever the id was configured to the MS Outlook, to the successor prior to moving out of the office.
- 2.3.2** The successor shall need to get the password reset and outlook data file restored, wherever applicable, after taking over the post.
- 2.3.3** The Relieving Officer [in case no substitute is posted, the immediate subordinate authority with whom the charge of the office is going to rest] need to ensure that the assigned email id along with login credentials and respective latest Outlook data file, wherever applicable, is handed over and due mention to this effect shall be made in the Charge Report.
- 2.3.4** The above should be done mandatorily to prevent unauthorized access to an account.
- 2.3.5** However the user can continue to use his/her by name email id during his/her entire service/tenure in Department of Posts.
- 2.3.6** In case on transfer and/or moving from one position to another, user shall notify such move so that the sender is aware of such change.
- 2.3.7** In respect of 'by name' email id, if user on transfer and after relinquishing charge receives any mail related to the previous post held, he/ she should transfer the mail to the successor without fail and delay.
- 2.3.8** The above process needs to be followed without any exception.

2.4 Data Retention:

- 2.4.1** 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 "Junk Email\Trash" and "Probably Spam" folders after a specified time period by the IA.

2.4.2 Department of Posts reserves the right to revise the above retention policy with appropriate approvals and advance notice to the users.

2.5 Data Backup

2.5.1 The backup of the email data available at Data Centre shall be done on a regular basis as per the DoP Backup Policy by the IA to ensure timely recovery from a system failure/crash/loss impacting the service.

2.5.2 However each user is responsible for the individual emails stored in their desktops or in the relevant webmail folders. The DoP will not be responsible for any accidental deletion of e-mails by the user either stored in their desktops or by accessing their mail account stored in the email server.

2.5.3 E-mails lost as a result of wrong configuration of the local mail clients (e.g. Outlook/Eudora/Thunderbird etc.) will not be the responsibility of the DoP and it does not offer any service for restoration of lost data due to an action committed by the user. Hence users shall take due precaution.

2.5.4 In the eventuality of a disaster/calamity, all possible attempts to restore services and content will be done. However, in circumstances beyond the control of DoP, it would not be held responsible for loss of data and services.

2.6 Desktop Protection

2.6.1 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-mails. Whilst these filters are constantly updated, the IA cannot guarantee that it shall provide 100% protection against all viruses and spam. Hence users are advised to mark as Junk or SPAM using this option available in the email application, if they consider so, any mail received in their mail box and also forward such mails to dop.spamreport@indiapost.gov.in for further necessary action by IA.

2.6.2 It shall be the responsibility of the Users using the desktop/laptop/handheld devices to ensure that all recommended best practices, issued from time to time, are followed without fail.

2.6.3 If email clients like outlook, thunderbird etc. are used, the user should take proper care of the desktop/laptop/mobile or other device in such a way that he/she shall comply with the terms and conditions of the DOP email Policy.

2.7 Deactivation of Accounts:

2.7.1 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. Subsequent to deactivation, the concerned user and the competent authority/nodal officer shall be informed.

2.7.2 A user account will be deactivated under the following circumstances and handled as stated below:

- i. The officer retires from service:** The officer would need to surrender his/her name based email account prior to getting relieved from the service. The IA based on the DoB given in the service book should identify the date of superannuation. However in case of resignation and voluntary retirement it is mandatory for the officer to inform the implementing agency of his/her resignation/voluntary retirement at least one week before the date of voluntary retirement/resignation.
 - a.** As email is a very crucial identity of an employee and is used everywhere (including their bank account, pension account etc.) and deactivation will create inconvenience for the officer. Officers of Department of Posts, who superannuate shall be allowed to retain the email account assigned in their name for **Six Months**, post superannuation. It is expected that within this **Six Months**, the user will change the e-mail address at all places as required by him/her. During this **06 months**, if this 'by name' email account is not used for a period of 90 days, the account will be deactivated and no request for activation will be accepted.
 - b.** The officer while communicating through the 'by name' email id after retirement and during the retention period should indicate "Retired" after his name in the Signature portion of the email.
 - c.** Retention of an email account does not entail an employee for any remuneration.
 - d.** The use of email account post retirement will be governed by the current policy and subsequent updates of the same.

- ii. **The officer resigns from service:** The officer would need to surrender his/her name based email account prior to getting relieved from the service. Department of Posts will introduce a component of getting clearance from the Nodal Officer identified for the purpose of e-mail service as part of their "No-Dues" form that is submitted by the individual prior to his/her resignation.
- iii. **The officer is no longer in a position to perform his duties (e.g. death / missing etc.):** The controlling officer will inform the IA.
- iv. **Inactive Account:** Any account which is inactive for a period of 90 days will be deactivated. The user id along with the data will be removed from the e-mail system after a period of 180 days & archived, if no request for activation is received during this period. Subsequently, all formalities will need to be completed for reopening of the said account with the same ID, subject to availability. In such cases, data from the backup may not be restored.
- v. **Violation of Policy or Misuse of Account:** It is the mandate of the IA to deactivate the email account if any policy violation or misuse of account is noticed under intimation to the Nodal Officer. The Nodal Officer will in turn inform the Controlling Authority of the user concerned for taking appropriate action as deemed fit.

2.7.3 Based on the conditions above, and as per the status of the officer, Competent Authority shall introduce a process to ensure that e-mail id is either deactivated/password changed, prior to giving "no-dues" to a user.

2.8 Status of account in case of Resignation or Superannuation:

2.8.1 The implementing agency would take action and accordingly change the user's by name email account status as "Superannuated/Resigned" as the case may be, after receiving the information and/or based on the data available in the system, with effect from date next to the date of superannuation/Resignation and without waiting for the completion of the retention period. The Controlling Officer should confirm from the IA before giving a No-Due certificate to the officer and the retirement benefits are processed.

2.8.2 The functional email ids assigned to the officer superannuating/retiring shall be processed as mentioned in Para 2.3 above.

2.8.3 If an officer retires or resigns or otherwise leaves the Department, the additional privileges such as group emailing privileges, if any assigned to the email account will be withdrawn immediately.

3. Recommended Best Practices: Users are advised to adopt the following best practices for safe usage of e-mail services:

3.1 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 Annexure - 1 to the DoP Email Policy. This application helps in making users aware of any unauthorized access to their account.

3.2 Users are strongly recommended to change their passwords on a periodic basis or as per the Password Policy.

3.3 Users must logout from their mail accounts whenever they leave the computer unattended for a considerable period of time. The user should log out from web based services like web email before closing the browser session. The email application has an auto logout feature that is triggered after a pre-defined period of inactivity.

3.4 The files downloaded from the internet or accessed from the portable storage media should be scanned for malicious contents before use. To ensure integrity of the downloaded files, digital signatures/hash values should be verified wherever possible.

3.5 Before accepting an SSL^[2] Certificate, the user should verify the authenticity of the certificate. User should type the complete URL^[3] for accessing the emails rather than click on a mail link for access. This is recommended to avoid phishing attacks.

3.6 Users should disregard any mail that requests details like login ID and password and should refrain from sharing such details over mail or otherwise with anyone.

3.7 After completing the activity in the current web based application, the browser session should be closed.

3.8 Emails identified as SPAM are delivered in the "Probably Spam" folder that exists in the user's mail box. Hence, users are advised to check the "Probably Spam" folder on a daily basis.

- 3.9** Sending an email 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 anti-virus software on the computer to prevent infection from USB drives, CDs or DVDs. It is also mandatory to ensure that the desktop operating system has the latest operating system patches for all software loaded. Such anti-viruses must be updated regularly. 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.
- 3.10** Attachments should be opened only when the user is sure of the nature of the email. If any doubt exists, the user should contact the sender to verify the authenticity of the e-mail and/or the attachment.
- 3.11** It is strongly recommended that the users use the latest version of their internet browser for safe browsing. The “save password” and auto complete features of the browser should be disabled.
- 3.12** 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.
- 3.13** User should use due discretion while creating classified and sensitive document. Unless required otherwise, the documents should be created in a manner that it cannot be edited.
- 3.14** Users should not open emails from dubious sources.
- 3.15** 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.
- 3.16** Password used for online forms/services/registrations/subscriptions should not be the same as the password of official E-mail account.
- 3.17** Users should take periodical (recommended weekly) backup of the Outlook Data file of their mail box and keep it in such a secured manner so that it can be used for restoration of email messages in the event of any unforeseen irreparable damage to the Desktop/laptop in which the mail box is configured to Outlook Client.

= = = / = = =

**GOVERNMENT OF INDIA
MINISTRY OF INFORMATION & COMMUNICATION TECHNOLOGY
DEPARTMENT OF POSTS**

Application Form for Creation of Email Account over India Post Domain

1. Type of Email Account (*Refer Para 1 under Guidelines*):.....
2. In case of Name Based Id:
 - i. Name of the Employee:
 - a) First Name:.....
 - b) Middle Name:.....
 - c) Last Name:.....
 - ii. Date of Birth (DD /MM/YYYY):.....
 - iii. Group (A/B/C/D):
 - iv. GPF / PRAN Number:.....
 - v. Designation:.....
 - vi. Contact Number (Mobile):.....
3. In case of all other type of Email Account:
 - i. Brief Details of Email Account Type:.....
.....
 - ii. Name & Designation of Current User:.....
 - iii. Contact Number (LL & Mobile) of Current User:.....
4. "xyz@indiapost.gov.in" OR "xyz.dop@nic.in" domain id, if any, remember to have used earlier for the purpose this application is made:.....
5. Circle Name:.....
6. Deployed Office WEG Code:.....
7. Deployed Office Name:.....
8. Remarks, if any:.....
9. Declaration: This is to declare that I have read & understand the Email Policy of Department of Posts along with its Annexures (revised from time to time) and I agree to be abide by it.

(Signature of Applicant)
Designation Seal of Applicant:.....

For Use by Controlling Officer:

10. Recommendations of Controlling Officer:.....
.....

11. It is certified that all the details mentioned by the applicant is correct as per records.

(Signature of Controlling Officer)
Designation Seal:.....

For Use by Nodal Officer:

12. Comment on the eligibility for the email id applied for:.....

13. Approval / Exception Approval of Competent Authority, wherever applicable:.....
.....

14. Email Id Nomenclature:.....

15. Email id Display Name:.....

16. Process of Rollout of Email Id to User by the IA:

17. Any other action item for IA:

(Signature of Nodal Officer)
Date:.....

For Use by Implementing Agency:

18. Status of Creation of Email Id as per Nomenclature & Display Name:.....
.....

19. Status of Rollout of Email Id to the User along with Date:.....

20. Status in respect of Other Action Items along with Date:

(Signature of IA Identified Person)
Name:
Date:.....

Guidelines / Terms & Conditions

1. All concerned may please use only CAPITAL LETTERS while filling up this form.

2. **Type of Email Account** may be one of the followings:
 - a. 'Name Based Id';
 - b. Functional Ids"
 - i. 'Designation Based Id';
 - ii. 'Office Based Id';
 - iii. 'Branch / Section in an Office';
 - iv. 'Specific Purpose Ids';
 - v. 'Any Other Category' (details to be mentioned).

3. The nomenclature & display name of the email id shall be decided by the Nodal Officer based on the current email policy. Applicant may refer to the email policy for details.

4. **Manner of Submission** of Application Form:
 - a. The applicant will input relevant details against Para 1, 2 or 3 (as applicable) & 4 to 9, sign and submit it to the Controlling Officer in hard copy.
 - b. The Controlling Officer will input relevant details against Para 10 & 11, authenticate it with his/her signature & Designation Seal, scan the complete application form in 'pdf' format and send it to the Nodal Officer by email over mail id email.nodalofficer@indiapost.gov.in. While sending this application to nodal officer, the controlling officer will use his/her functional or by name India Post domain email id only and the subject line should preferably be as "Email Id Creation _ <Type> _ <Circle>". The Controlling Officer is defined in the Email Policy.
 - c. The Nodal Officer upon receipt of mail from Controlling Officer will scrutinize the application based on the existing email policy and take suitable necessary action. He will put relevant inputs under Para 12 to 17 and forward the application to IA's identified resource person/service desk (L1) for further necessary action.
 - d. The IA's identified resource person/service desk (L1) will take necessary action and will report compliance back to the Nodal Officer within the pre-defined time line. The compliance email will contain input from the IA's identified resource person/service desk against the Para(s) 18 to 20. Upon receipt of compliance from IA, Nodal Officer will update controlling officer concerned about completion of the activity.

5. The User shall be abide by all the terms & conditions of the DoP Email Policy revised from time to time without any exception unless an exception is otherwise approved by the Competent Authority.

= = = / = = =

GLOSSARY

SI	Term	Definition
1	Outsourced / Contractual Employees	An employee who works under contract of Gol. A contractual employee is hired for a specific job or assignment. A contractual employee does not become a regular addition to the Gol staff and is not considered as a permanent employee of Gol.
2	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.
3	URL	A URL (Uniform Resource Locator) 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.

END OF DOUCMENT

Annexure - 3 to the DoP Email Policy V.1.0

DoP Password Policy V.1.0

- 1. Purpose:** The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.
- 2. Scope:** The scope of this policy includes all end-users of DoP email services and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the India Post domain. These include personnel with their designated desktop systems/laptops. The scope also includes designers and developers of individual applications.

3. Policy:

3.1 Policy Statements:

3.1.1 For users having accounts for accessing systems/services:

- 3.1.1.1** Users shall be responsible for all activity performed with their personal user Ids. Users shall not permit others to perform any activity with their user Ids or perform any activity with Ids belonging to other users.
- 3.1.1.2** All user-level passwords (e.g. email, web, desktop computer etc.) shall be changed periodically. Presently the email password expiry period is configured as 90 days. Similar expiry limit will be imposed on other applications in future. The IA of the respective application will suitably notify to the users about expiry of the password well in advance. In such case the users are required to change the password. Users shall not be able to reuse previous passwords.
- 3.1.1.3** The password expiry period is subject to revision by the competent authority.
- 3.1.1.4** For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.
- 3.1.1.5** Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

- 3.1.1.6** All access codes including user ID passwords, network passwords, PINs etc. shall be treated as sensitive and confidential information and not be shared with anyone, including personal assistants or secretaries.
- 3.1.1.7** All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.
- 3.1.1.8** Passwords must not be communicated through email messages or other forms of electronic communication such as phone to anyone.
- 3.1.1.9** Passwords shall not be revealed on questionnaires or security forms.
- 3.1.1.10** Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
- 3.1.1.11** The same password shall not be used for each of the systems / applications to which an user has been granted access e.g. separate password to be used for a Windows account and an UNIX account.
- 3.1.1.12** The "Remember Password" feature of browser/applications shall not be used.
- 3.1.1.13** Users shall refuse all offers by software to place a cookies on their computer such that they can automatically log on the next time when they visit a particular Internet site.
- 3.1.1.14** First time login to systems / services with administrator created passwords, should force changing of password by the user.
- 3.1.1.15** If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
- 3.1.1.16** The password shall be changed immediately if the password is suspected of being disclosed or known to have been disclosed to an unauthorized party.
- 3.1.1.17** Users must not be able to reuse their last 5 passwords when choosing a new password.
- 3.1.1.18** Users must be locked out for next 30 minutes after 5 successive failed logon attempts due to incorrect user id/password.

3.1.1.19 Password should comply with the standards as specified in Para 3.2.

3.1.2 For designers/developers of applications / sites:

3.1.2.1 No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

3.1.2.2 The backend database shall store hash of the individual passwords and never passwords in readable form.

3.1.2.3 Password should comply with the standards as specified in Para 3.2.

3.1.2.4 Users shall be required to change their password periodically and not be able to reuse last 05 passwords.

3.1.2.5 For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

3.2 Policy for constructing a password: All user-level and system-level passwords must conform to the following general guidelines described below:

3.2.1 The password shall contain more than eight characters.

3.2.2 The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# \$%^&*()_+|~-=\`{}[]:~<>?,./).

3.2.3 The password shall not be a word found in a dictionary (English or foreign).

3.2.4 The password shall never be the same as the Login Id / User Name as well as not be a derivative of the user ID, e.g. <username>123. It should also not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

3.2.5 The password shall not be a slang, dialect, jargon etc.

3.2.6 The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters etc.

3.2.7 The password shall not be based on computer terms and names, commands, sites, companies, hardware and software.

3.2.8 The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

3.2.9 The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321 etc. or any of the above spelled backwards.

3.2.10 The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).

3.2.11 Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

3.3 Suggestions for choosing passwords: Passwords may be chosen such that they are difficult-to-guess yet easy-to-remember. Methods such as the following may be employed:

3.3.1 String together several words to form a pass-phrase as a password.

3.3.2 Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.

3.3.3 Combine punctuation and/or numbers with a regular word.

3.3.4 Create acronyms from words in a song, a poem or any other known sequence of words.

3.3.5 Bump characters in a word a certain number of letters up or down the alphabet.

3.3.6 Shift a word up, down, left or right one row on the keyboard.

4 Responsibilities:

4.1 All individual users having accounts for accessing systems/services in the India Post domain and system/network administrators of DoP servers/network equipments shall ensure implementation of and compliance to this policy.

4.2 All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

5 Compliance:

5.1 Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.

5.2 Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

= = = / = = =