

**केन्द्रीय सूचना आयोग**  
**Central Information Commission**  
2तल ,विंग /'B'2nd Floor, 'B' Wing  
अगस्त क्रांति भवन/ August Kranti Bhawan,  
भिकाजी कामप्लेस/Bhikaji Cama Place  
नई दिल्ली/New Delhi 110066

F.No.28/JS(Law)/Email/CIC/2016

Dated 7 September 2016

**E-mail Usage policy of Central Information Commission**

1. The objective of this policy is to ensure secure access and usage of Government of India 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 Government of India e-mail service, amount to the user's agreement to be governed by the policy of Government of India in this regard. Any other policies, guidelines or instruction on e-mails previously issued in this Commission will be suspended by this policy.
2. Government of India has formulated the "E-mail Policy of Government of India " which has been issued vide F.no. 2(22)/2013-EG-II, dated 18 February 2015 in Gazette of India, published on 19 February 2015. Guidelines for "E-mail Account Management and Effective E-mail Usage" has been released by Ministry of Communication and Information Technology vide F.No. 2(22)/2013-EG-II in October 2014. National Information Centre has issued precautions for messaging services (version 0.1). Directions for 'Safe Email' are also placed on e-mail portal of @Gov.in.
3. Following best practices are exacted from "Guidelines for E-mail Account Management and Effective E-mail usage" issued by Ministry of Communications and Information Technology, Government of India for convenience of reference /use in the Central Information Commission.
  - a. The User is responsible for any data/e-mail that is transmitted using the GOI e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
  - b. Other than Government website, 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.
  - c. 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.



- d. 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.
  - e. Users should not open e-mails from dubious sources.
  - f. To ensure integrity of the downloaded files, digital signatures/ hash values should be verified wherever possible.
  - g. User should exercise caution in opening mails where links are embedded in the mail. The authenticity and the safe nature of the links should be ascertained before clicking the link.
4. Advice from "Safe-email" on e-mail website(@Gov.in), is reproduced.

**"9. Never open/ respond any mail/ attachment from unknown sender.**

If it happens that a few spam mails do manage to sneak through, make it a must to delete all them. Replying /Opening such emails/ attachments typically only informs the sender that they have found an active email address to send more spam emails or They may contain what are known as "letter bombs" or "viruses," which can damage your PC."

5. Following precautions are re-iterated from "Electronic Mail Usage Guidelines" issued by National Informatics Centre:
- a. To counter the problems associated with virus/ worms, which are normally destructive in nature, the recipient of the e-mail should not open any of the attachments enclosed to the e-mail without verifying the authenticity of the sender of the e-mail. Certain viruses/ worms become active at the predefined time. They remain silent for rest of the period. Although Anti-Virus tools are normally deployed at the Mail Gateways and Mail Servers, sometimes they become ineffective to a new virus/ worm, for which these tools do not have a cure yet. Therefore, it is always recommended to clean up the mailbox so that there is no unwanted e-mail in any of the folder / inbox.
  - b. It is recommended not to use the mailbox as the repository for sensitive/ useful data. It has been observed that the users keep huge number of files in the mail store as if it is a vaulting facility for their data/ communications in electronic form. There may be a time bomb (time triggered destructive virus) sitting inside the mail store to destroy your data at a pre-defined time defined by the virus designer.



6. The security audit of NIC network infrastructure shall be conducted periodically by NIC cell with Central Information Commission. Deviations shall be brought to notice.
7. This guidelines is an abstract of the Government of India/ NIC policies with regard to use of e-mail service provided by Government of India/ NIC. This guideline does not in any way supersede the GOI/NIC guidelines which continue to be applicable fully.
8. This has the approval of Chief Information Commissioner.

*Y. Singhal*

(Yogesh Kumar Singhal)  
Joint Secretary(Law)  
Tel No. 26181925

Copy to:

- 1) PPS to CIC *8/9/16*
  - 2) PS to IC(BS) *7/9*
  - 3) PS to IC(YA) *7/9*
  - 4) PS to IC(SH) *7/9*
  - 5) PS to IC(MP) *7/9*
  - 6) PS to IC(KY) *7/9*
  - 7) PS to IC(SA) *7/9/16*
  - 8) PS to IC(SB) *7/9*
  - 9) PS to IC(BJ) *7/9*
  - 10) PS to IC(DP) *7/9/16*
  - 11) PS to IC(AB) *7/9/16*
  - 12) PS to Secretary *7/9/16*
  - 13) PS to AS *7/9*
  - 14) PS to Registrar *7/9/16*
  - 15) JS(P&B)/ JS(Law)/ JS(MR)/JS(Admn) *7/9/16*
- 7/9/16*
- 7.09.16*

*o/c*