No. DIT-F(10)-3/2008-Vol-I-124
Department of Information Technology
Government of Himachal Pradesh

From

The Addl. Chief Secretary IT to the Government of Himachal Pradesh

To

All the Administrative Secretaries to the Government of Himachal Pradesh

Dated: Shimla-9, the 21st October, 2013

Subject: - Consideration of "E-Mail policy of GoI" & "Policy on acceptable use of IT Resources of GoI", formulated by DeitY, by the Committee of Secretaries.

Sir,

This is with reference to the email dated October 15, 2013 received from the DeitY, GoI on the subject cited above. Please find attached herewith a draft note for the Committee of Secretaries (COS) for considering the following policies, formulated by the DeitY, GoI:

i. E-Mail Policy of GoI
ii. Policy on Acceptable Use of IT Resources of GoI.

The recommendations are to be placed before the Committee under the chairmanship of Cabinet Secretary. It is, therefore, requested that comments of your department may be furnished by 29th October, 2013 to this department. A copy of the Policies is attached herewith at **Annexure-A** for reference please.

Yours sincerely,

Director,
Department of Information Technology,
Himachal Pradesh.

E-mail Policy

Of

Government of India

October 2013

Table of Contents

1. Introduction

1.1 E-mail is a major mode of communications for the entire Government. Communications include Government of India data that travels as part of mail transactions between users located in the country or anywhere in the world.

1.2 This policy of the Government of India (GOI) lays down the guidelines with respect to use of e-mail services. It is mandatory for all Government employees working under different arms of the Government, both Central and State, to use this e-mail service. The implementing agency [1] for this service is National Informatics Centre (NIC), under Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology.

2. Scope

2.1 E-mail services provided by GoI will only be used for official communications. The use of e-mail services from other service providers shall be strictly limited to non official/ personal communication. .

2.2 This policy is applicable to the employees of GOI and employees of those state governments that use the e-mail services of GOI and also those state governments that choose to adopt these policies in future. The directives contained in this policy are to be followed by all of them with no variations. All users of e-mail services can find further information in the supporting policies available on

http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy")

3. Objective

3.1 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, ethical and lawful manner. Use of the Government of India 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 Ministries/Departments/Offices/ Statutory Bodies /Autonomous bodies (henceforth referred to as "Organization[2]" in the policy) that draw their fund from the consolidated fund of India. Refer "NIC e-mail Services and Usage Policy" available on http://www.deity.gov.in/content/policiesguidelines/ under "E-mail Policy"

3.3 This Policy supersedes any other E-Mail policy previously issued.

4. Basic requirements for GoI e-mail Service

4.1 Security

4.1.1 In view of the security concerns governing a sensitive deployment like e-mail, apart from the service deployed by the implementing agency [1] there would not be any other e-mail service under Government of India.

4.1.2 All organizations shall initiate the process of migrating their mail services to the centralized deployment of the implementing agency [1], in case they are running their independent e-mail setup.

Correspondence regarding the same can be sent to support@gov.in.

4.1.3 For the purpose of continuity, all efforts would be made to ensure retention of e-mail addresses. Wherever it is technically feasible, data migration will also be done.

4.1.4 E-mail can be used part of the process to do electronic file processing in Government of India. Refer http://darpg.gov.in/darpgwebsite_cms/Document/file/CSMeOP_1st_Edition.pdf for more details

4.1.5 From the perspective of security, the following will be adhered to by all users of the Government of India e-mail service:

4.1.5.1 E-mail is considered an inherently insecure method of communication. There is no guarantee that the recipient of an e-mail is in fact genuine, nor is there any guarantee that the sender of e-mail is genuine. Therefore, use of DSC is mandatory for sending mails deemed as classified, confidential, secret or restricted. Where ever considered necessary such classified information may be transmitted using encryption and digital signature only..

4.1.5.2 It is strongly recommended that for Government of India officials stationed at Embassies or working in Missions or on deputations abroad, to only use static IP addresses/Virtual Private Networks(VPN)[6]/One Time Password (OTP)[5] for accessing the GOI e-mail services. This is imperative in view of the security concerns that exist in other countries.

4.1.5.3 Updating of current mobile number under the personal profile is mandatory for security reasons. The number

would be used only for alerts and information regarding security that would be sent by the implementing agency. Updation of personal e-mail id, in addition to the mobile number will also be required by the implementing agency in order to reach the user as an alternate means for sending alerts.

4.1.5.4 Users shall not download the e-mails from his/her official e-mail account, configured on the Government of India mail server by configuring POP[4] on any other service provider.

4.1.5.5 Any e-mail addressed to a user ,whose account has been deactivated/deleted due to Clause No 4.13 below ,will not be redirected to another e-mail address. Such e-mails may contain content that belongs to the GoI framework and hence no mail will be redirected.

4.1.5.6 Users must ensure that the access device (desktop/laptop/handset etc) have the latest operating system patches and application patches. They must also ensure that their handheld devices have the latest antivirus signatures.

4.1.5.7 As part of the security framework, in case a compromise of an id is detected, a SMS alert will 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 will be sent. Both the e-mail and the SMS will contain details of the action to be taken by the user. In case a user does not take the required action even after five SMS alerts (indicating a compromise), the

implementing agency reserves the right to reset the password of that particular id. In case of help, user can call the 24x7 helpdesk of the implementing agency or use the "Forgot Password" application to set a new password.

4.1.5.8 In case of a situation when a compromise of an id impacts the e-mail service /impacts data security or an input is received from the authorized investigating agency, the implementing agency will reset the password of a user id. This action will be taken on an immediate basis, and the information to the user shall be provided subsequently (over phone/SMS).

4.1.5.9 Forwarding of mail from the e-mail id provided by Government of India to a personal id outside the Government mail service is not allowed.

4.1.5.10 Auto-save of password in the Government mail service is not allowed and has not been provided as an option due to security reasons.

4.1.5.11 For more details regarding Security, refer "NIC Security Policy" for a user available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy".

4.2 Recommended Best Practices

4.2.1 All users must check their last login details while accessing their e-mail account by using the application created for this purpose. Refer "NIC Services and Usage Policy" available on http://www.deity.gov.in/content/policiesguidelines under "E-mail

Policy" . Checking the last login makes a user aware of any unauthorized access to his/her account.

4.2.2 Use of encryption and Digital Signature Certificate (DSC) [8] is recommended for sending any mail deemed as classified, confidential, secret or restricted.

4.2.3 It is mandatory for users stationed at sensitive offices to use OTP [5] for secure authentication.

4.2.4 It is strongly recommended to change passwords on a periodic basis or as per policy.

4.2.5 Users must logout from their mail accounts whenever they leave the computer unattended for a considerable period of time.

4.2.6 The official e-mail address must not be used to subscribe on any unsafe / fake website. Such websites may try to flood the inbox or spammers may try to send bulk spam [11] e-mails (which may contain virus).

4.2.7 The user shall use the latest version of Internet Browser.

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

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

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

4.2.11 Before accepting an SSL [7] certificate, the user should verify the authenticity of the certificate. User should type the complete URL [12] for accessing the e-mails rather than click on a mail link for access. This is recommended to avoid phishing [10] attacks.

4.2.12 The implementing agency (NIC) does not ask for details like login id and password over mail. Users should disregard any mail that requests for the same, and should refrain from sharing such details over mail with anyone.

4.2.13 The user should log out from web based services like web e-mail, before closing the browser session.

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

4.2.15 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 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's 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.

4.2.16 E-mails identified as Spam [11] are delivered in the "Probably Spam" folder that exists in the user's mailbox. Hence, users are advised to check the "Probably Spam" folder on a daily basis.

4.2.17 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.

4.3 Creation of E-mail Addresses

4.3.1 This policy extends to all employees of GOI and employees of those state governments that use the e-mail services of GOI and also those state governments that choose to adopt these policies in future.

4.3.2 Accounts for outsourced/contractual employees shall also be created after due authorization from competent authority of that particular organization. These accounts will be created with a pre-defined expiry date.

4.3.3 E-mail id's can be created based on both name and designation. It is advisable for an official to create two ids, one based on his/her designation and the other based on his/her name.

4.4 Process of Account Creation

4.4.1 An e-mail account has to be created for every employee in an organisation. The user needs to request for an account by filling out the form available on the e-mail site and send it to the nodal officer of respective organization [2].

4.4.2 The account creation process is initiated after due authorization by the Competent Authority.

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

If any user department wants to adopt an addressing policy that represents their department, they can inform the implementing agency [1]. However "id" uniqueness needs to be maintained. Hence prior to sending a request for "id" creation users are requested to use the

"idlookup" tool available on the implementing agency's[1] e-mail site to ensure "id" availability.

4.5 Process of handover of designation based e-mail id's

4.5.1 The official id should be handed over to the successor and the official can continue to use his/her personal id during his/her entire tenure in Government of India.

4.5.2 Prior to leaving an organization on transfer, the officer to whom the official id had been assigned should ensure that the password for the id i**s** changed. His successor will need to get the password reset once he takes over the post.

4.5.3 The above must be mandatorily done to prevent unauthorized access to an account.

4.5.4 The nodal officer in each organization [2] needs to ensure that the password is changed prior to giving "No-Dues" to the officer. The password will be reset by the successor.

4.5.5 The above process needs to be followed without any exception. If an id is misused, the respective nodal officer of each organization [2] will be held accountable.

4.5.6 The user needs to inform the implementing agency[1] prior to his superannuation/transfer or send a mail informing the same to support@gov.in

4.6 Delegated admin console

4.6.1 Organizations that avail the delegated admin console service from the implementing agency [1] can use the same to provision the process of account creation/ deletion/ password change of user "Id's" under that respective domain themselves as and

when required. Refer NIC e-mail services & Usage Policy available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy" for more details.

4.6.2 Organizations [2] that do not opt for the admin console need to forward their request to the implementing agency's support cell (support@gov.in). Forms should be complete in all respects for the account to be created. Time taken to create a single account is one working day. For bulk creation of accounts (up to 20) will take a minimum of 2 working days and if the list of accounts exceeds 100, support can take up to a maximum of 5 working days to respond.

4.7 E-mail Domain & Virtual Hosting

4.7.1 GoI provides virtual domain hosting for e-mail. If an organization so desires, the implementing agency [1] can offer a domain of an e-mail address as required by them. This implies that if an organization requires an address as per the website that they are operating on, the implementing agency [1] can provide the same.

4.7.2 By default the address "userid@gov.in" will be assigned to the users. The user id will be created as per the addressing policy (refer NIC Policy on Format of e-mail addresses available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy"). Users requesting for an "id" need to ensure that it is unique and available.

4.7.3 Users desirous of an address belonging to other domains (like xxxx@deity.gov.in, yyyy@tourism.gov.in) need to forward their request through their competent authority.

4.8 Use of Secure Passwords

4.8.1 All the users accessing the e-mail services must use strong passwords for security of their e-mail accounts. In this regard please refer to the "Password policy" available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy".

4.9 Privacy

4.9.1 The user should ensure that e-mails are kept as confidential. Implementing agency [1] will take all possible precautions on maintaining privacy. User must ensure that information regarding his/her password or any other personal information is not shared with anyone.

4.10 Scrutiny of e-mails/Release of logs

4.10.1 Notwithstanding anything in the above clause, ICERT, NTRO and any other agency that is authorized by Government of India for this purpose can, under exceptional circumstances request the implementing agency[1] for e-mails / logs and correspondences in connection with matters relating to national security or abuse incidents or violations of other policies.

4.10.2 The implementing agency [1] will provide the necessary cooperation to such agencies when approached through authorized channel. The consent of the user in this regard will not be taken.

4.10.3 The implementing agency [1] will not accept request from any other organisation for scrutiny of e-mails/Release of logs.

4.11 Data Retention

4.11.1 Individuals 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 will be automatically purged from folders mentioned below after the time periods as shown:

- Trash (deleted e-mails) - 7 days
- Probably Spam (unsolicited e-mails) – 7 days

4.11.2 The implementing agency [1] reserves the right to revise the above retention policies with appropriate approvals and advance notice to the users.

4.12 Data Backup

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

4.12.2 Each user is responsible for the individual e-mails stored in their folders. The implementing agency [1] will not be responsible for any accidental deletion of e-mails by the user.

4.12.3 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 implementing agency [1].

4.12.4 The implementing agency [1], does not offer a service for restoration of lost data due to an action committed by the user.

4.12.5 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 the implementing agency [1], it would not be held responsible for loss of data and

services. For disaster recovery and Business Continuity please refer to "NIC Services and Usage Policy" available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy".

4.13 Deactivation of accounts

An account will be Expired/Deactivated or deleted under the following conditions:

4.13.1 The officer retires from Service: The officer would need to surrender his/her official designation based account prior to getting relieved from the service. However name based e-mail addresses can be retained as per the conditions defined in section 6.2 for details. It is mandatory for the officer to inform the implementing agency/support@gov.in of his/her superannuation.

4.13.2 The officer resigns from service: The officer would need to surrender his/her official account prior to getting relieved from the service. Each organisation will introduce a component of getting clearance from the respective 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. Refer 6.3 for details.

4.13.3 The officer is no longer in a position to perform his duties (death/missing etc). The nodal officer of that respective organization [2] needs to take necessary action as mentioned above.

4.13.4 Inactive account: Any account which is inactive for a period of 90 days will be deactivated. The userid along with the data will

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 will 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 will not be restored.

4.13.5 Violation of policy: It is the mandate of authorized personnel across all organizations at the Central and the State level under whose request the account has been created, to inform the support cell of the implementing agency [1] when any of the above conditions is triggered. Intimation needs to be sent to support@gov.in.

4.13.6 Misuse of account: In case information is not sent or sent at a later date, the implementing agency [1] will not be responsible in case the account is misused and comes under scrutiny of the designated investigating agencies.

4.14 Desktop Protection

4.14.1 Spam [11] filters and anti-virus filters have been configured at the e-mail gateways by the implementing agency [1]. These filters are there to protect the e-mail setup from viruses and unsolicited e-mail. Whilst these filters are constantly updated, the implementing agency [1] cannot guarantee that it will provide 100% protection against all viruses and spam [11].

4.14.2 It is the responsibility of the person who is using the desktop/laptop/handheld devices to ensure that all recommended best practices are followed from time to time.

4.15 Security Incident Management Process

4.15.1 An incident response and management is necessary for detecting security incidents, minimizing loss and damage, mitigating the weaknesses that were exploited and restoring information assets in a timely manner.

4.15.2 This process is applicable to all policy violations reported by the Administrator or the Users.

4.15.3 The implementing agency[1] reserves the right to deactivate/remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the system

4.15.4 Any such incident must immediately be brought to the notice of the ICERT and the implementing agency [1] as per the guidelines laid down in the Cyber Security Policy of Government of India.

4.15.5 A security incident is defined as any adverse event which occurs on any part of the e-mail services which affects data, resulting in;

4.15.5.1 Compromise of a user account

4.15.5.2 Violation of this policy thereby causing a security breach

4.15.5.3 Loss of portable storage media containing Government data

4.15.5.4 Detection of a phishing[10] site of the e-mail service of Government of India

4.15.5.5 Spread of Spam/Virus that effect the system and service.

4.15.5.6 Any other consequence affecting the security of the e-mail services

4.16 Service Level Agreement

4.16.1 The implementing agency [1] will provide the e-mail service based on the Service level agreement of the implementing agency available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy.

4.17 Complaint Registration

4.17.1 The implementing agency [1] operates a 24x7 Support cell for complaint registration and for providing online support. Subsequent to complaint registration, a ticket is issued and the approximate time for problem resolution is given to the person registering the complaint.

4.17.2 Complaint can also be registered by sending a mail to support@gov.in

5. Roles required for the Policy

5.1 Roles required for the implementation of the policy

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

5.1.1 Competent Authority as identified by each Organization[2]

5.1.2 Designated nodal officer identified by each Organization[2]

5.1.3 Implementing agency i.e. National Informatics Centre

6. Responsibility of respective organizations

This section of the policy aims at providing secure and acceptable use of the e-mail system by the respective organizations under Government of India and State Government.

6.1 All organizations [2] shall implement appropriate controls to ensure compliance to e-mail policy for user, and e-mail policy for their respective setup.

6.1.1 The concerned organization [2] as indicated above shall ensure that official e-mail accounts of its users are created only on the mail server of the implementing agency [1].

6.1.2 E-mail policy and the related documents shall be disseminated to the concerned officials.

6.1.3 Nodal officer of the particular organization [2] shall ensure resolutions of all incidents related to the security aspect of e-mail policy.

6.1.4 Competent Authority of that particular organization [2] shall ensure that e-mail security trainings are arranged at regular intervals. The implementing agency [1] shall provide the required support.

6.2 Status of account in case of Resignation or superannuation

6.2.1 Every personnel/officer at the time of his resignation or superannuation must inform the concerned nodal officer / implementing agency [1] regarding his resignation or superannuation through the competent authority.

6.2.2 The nodal officer / implementing agency would take an action and accordingly change the officers account status. This should be made mandatory before the concerned organization [2] gives

a No-Due certificate to the officer and the retirement benefits are processed.

6.2.3 However, e-mail is a very crucial identity of an employee, and is used everywhere (including his bank account, pension account etc.) Deactivation [3] will create inconvenience for the officer. In view of the same, officers of Govt. of India, both at the centre and state 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 name for one year, post resignation or superannuation.

6.2.4 The designation based id will be processed as mentioned in point no 4.5 above. It is expected that within this one year the officer will change the e-mail address at all places as required by him. During this one year if the personal account is not used for a period of 90 days, the account will be deleted and no request for activation will be accepted.

6.2.5 It is mandatory for the concerned user to inform the implementing agency by sending a mail to support@gov.in of his resignation or superannuation as the id status will be changed, post resignation or retirement. The use of his account will be governed by the current policy and subsequent updates of the same.

6.2.6 Retention of an account does not entail an employee for any remuneration.

6.2.7 In case an officer resigns from service before completion of 20 years, his/her personal account will be deleted as part of the No-Dues process. This needs to be ensured by the competent

authority of each organization and the implementing agency [1] accordingly should be informed.

6.3 Policy Dissemination Guidelines:

6.3.1 E-mail policy dissemination activity involves distribution of the policy and all its relevant documents to the respective users.

6.3.2 Users should be aware of the e-mail policy. Thus the Department should ensure the availability of the e-mail policy to the users. This document provides guidelines to disseminate the e-mail policy.

6.3.3 The dissemination of the e-mail policy should be ensured by the Head of the concerned Department/Organization.

6.3.4 Read only access should be given to the intended users.

6.3.5 Training and awareness programmes on the e-mail policy should be organized periodically.

6.3.6 Newsletters, banners, bulletin boards etc should be used to facilitate increased awareness on the e-mail policy.

6.3.7 Employee orientation program should include a session on the e-mail policy.

7. Responsibility of a User:

7.1 The "E-mail Policy of Government of India" aims to provide guidelines for secure and acceptable use of e-mail services by the users.

7.2 Acceptable use of E-mail Policy:

7.2.1 E-mail is provided as a professional resource to assist users in fulfilling their official duties. Hence the use of the e-mail

account must be ideally restricted to official correspondences only, however personal e-mails can be sent and received as long as the service is not put to any use which is considered inappropriate or impinges on National Security or violates any policy of the Government.

7.2.2 Examples of inappropriate use:

7.2.2.1 The creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

7.2.2.2 The unauthorized exchange of proprietary information or any other privileged, confidential sensitive information.

7.2.2.3 Users shall not attempt any unauthorized access of the services. Unauthorized access includes, for example, the distribution of e-mails anonymously, use of other officers' user-ids or using a false identity.

7.2.2.4 The creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

7.2.2.5 The creation and exchange of information in violation of any laws, including copyright laws.

7.2.2.6 Willful transmission of an e-mail containing a computer virus.

7.2.2.7 The misrepresentation of the identity of the sender of an e-mail.

7.2.2.8 The use or attempt to use the accounts of others without their permission.

7.2.2.9 Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sex etc.

7.2.2.10 Exchange of e-mails containing Anti-National Messages.

7.2.2.11 Sending personal e-mails to a broadcast list. The implementing agency [1] does not allow use of distribution lists for the purpose of sending e-mails that are personal in nature, such as, season greetings, personal functions etc.

7.2.3 Any case of inappropriate use will be considered a violation of the policy and may result in disciplinary action as deemed appropriate. Further such instances would also invite scrutiny by the investigating agencies depending on the nature of violation.

7.3 User Responsibility:

7.3.1 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. Sharing of passwords is not recommended.

7.3.2 Each individual is responsible for his/her account, including the safeguarding of access to the account. An e-mail originating from an account is deemed to be authored by the account owner, and it is the responsibility of the owner to ensure compliance with these guidelines. The user's responsibility shall extend to the following:

7.3.2.1 User shall be responsible for the activities carried out on the client system, using the accounts assigned to him.

7.3.2.2 Official e-mail shall not be forwarded to the personal e-mail account.

7.3.2.3 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.

7.3.2.4 Users shall ensure that all the access devices (Handheld Devices/ Desktops/ Laptops etc.) used for this purpose are updated regularly with respect to various security patches and anti-virus signatures.

7.3.2.5 User's network access shall be subjected to monitoring/filtering for malicious/unauthorized activities.

7.3.2.6 Back up of important files shall be taken by the user at regular intervals. The implementing agency [1] will not restore lost data for a user caused due to his/her action.

7.3.2.7 User shall report any security incident to the System Administrator of the implementing agency[1] by sending a mail to support@gov.in

7.3.2.8 Informing the designated nodal officer / implementing agency at the time of superannuation/transfer.

8. Exception Management

8.1 For any special permission/exception, the user shall take approval from the competent Authority of his respective organization [2]. The request will be routed through the implementing agency [1] subsequent to approval from the Competent Authority of that respective organization [2].

9. Review

9.1 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:

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

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

10. Enforcement

10.1 This "E-mail policy" is applicable to all employees of GOI and employees of those state governments that use the e-mail services of GOI and also those state governments that choose to adopt these policies in future. It is mandatory for all users to adhere to the guidelines of the policy without exception.

GLOSSARY

S.No	TERM	DEFINITION
1.	**Implementing agency**	For the purpose of this policy, the implementing agency is "National Informatics Centre"
2	**Organization**	For the purpose of this policy, organization refers to all Ministries/Departments/Offices/Statutory Bodies/Autonomous bodies/ , both at the Central and State level
3	**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
4	**POP**	**POP i**s short for ***P****ost* ***O****ffice* ***P****rotocol,* a protocol used to retrieve e-mail from a mail server
5	**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
6	**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
7	**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.
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	**Cookies**	**Cookies** are small files which are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular

		user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next.
10	**Phishing**	**Phishing** is a fraudulent attempt, usually made through e-mail, to steal a user's personal information. 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, 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. 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**.**
11.	**SPAM**	**Spam** is the use of e-mail systems to send unsolicited bulk e-mails, especially advertising, indiscriminately.

12.	**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.

Policy on Acceptable Use of IT Resources

Of

Government of India

October 2013

Table of Contents

1. Introduction

1.1 The IT resources are supposed to increase employee productivity and are important tools for the Government. IT as a resource is provided to a Government employee as an aid to process information for his area of work. However, the misuse and abuse of the Government's IT resources can all but eliminate the advantages of having them and may result in unwanted risk and liability for the Government. IT resources provide access to plethoric information which helps a Government Official do his job and be well-informed. The facilities that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc.

1.2 This Policy on Acceptable Use of IT Resources is designed to help a user understand the expectations for the use of those resources, and to help them use those resources wisely. The IT resources provided to a user have a significant cost and that means the Government expects an Official to use the resources primarily for government-related purposes.

1.3 With the above background, arose the need for creation of a Policy on Acceptable Use of IT Resources which would apply to all users. The creation of this policy is in consonance with international best practices. This policy is intended to provide a framework for use of Information Technology resources provided by the Government. It applies to all computing, telecommunication and network facilities provided by the Government. This Policy on Acceptable Use of IT Resources is established with the following objectives:

1.3.1 To establish appropriate and acceptable practices regarding the use of Information Technology resources.

1.3.2 To document the responsibilities and obligations of the users who may use the Government information resources.

1.4 Government of India provides access to the Government's IT Resources for its employees, contractual employees and other authorized workers, collectively referred to as "users" working across various Ministries/Departments/Statutory Bodies/Autonomous Bodies, referred to as "Organisation" under both Central and State Government.

1.5 This Policy on Acceptable Use of IT Resources governs all electronic activity of users using and accessing the Government's IT resources such as Internet

Services, Government e-mail and Government provided access to the Internet, and applies to the use of the Government's Information Technology Services both on and off Government property.

1.6 "The Government's IT Resources" means Government provided devices, Internet connections (including wireless connections) provided by the Government, Government provided e-mail accounts, intranet and any remote connection to Government systems. A user is deemed to access and use the Government's IT resources through any electronic activity conducted on the Government's Network using any device (whether or not such device is a Government provided device) regardless of the user's physical location.

1.7 Government provided devices" means any electronic device provided by the Government, including, but not limited to, desktop computers, laptops, and hand-held devices, such as personal digital assistants (PDAs), smart phones, iPads, and tablets

1.8 By using the Government Department's IT Resources, a user agrees to follow this policy and all applicable Government, policies and guidelines. All users must report any misuse of the IT resources or receipt of any communication that violates this policy to authorized authority as mentioned in the policy.

2. Purpose

The purpose of this policy is to outline the acceptable use of IT resources provided by the Government to its users. This policy is in place to protect the employee and cyber framework of Government of India. Inappropriate use a resource exposes the framework to risks including virus attacks, compromise of network systems and services, and legal issues. The policy applies to all IT resources and includes:

2.1 Network access,
2.2 E-mail access,
2.3 Access to social media,
2.4 Use of devices issued by Government of India to an officer for official use etc

3. Scope

This policy applies to employees, contractors and Consultants of Government of India, including all personnel affiliated with third parties. This policy applies to all resources (Network access, Email services, access to social network, use of external storage etc) that is owned or leased by Government of India The personnel mentioned above are expected to be familiar with and to comply with this policy, and are also required

to use their common sense and exercise their good judgment while using the resources offered by Government of India. The Policy applies to all IT devices and includes:

3.1 Computers and desktop devices
3.2 Portable devices such as laptops and mobiles
3.3 External storage devices
3.4 PDAs and tablets that have been provided by the Government.
3.5 Personally-owned devices connected to ACT Government resources and
3.6 Network resources like internet connections,(including wireless connections),email accounts, intranet and any other remote connections to Govt. system.

4. Objective

The objective of this policy is to ensure the “Proper access and usage of Government of India IT resources” by its users. Users have the responsibility to use these resources in an efficient, effective, ethical and lawful manner. Use of resources offered by Government of India implies user's agreement to be governed by this policy.

5. Roles and Responsibilities

Roles required for the implementation of the policy: The following roles are required under each Department/Ministry/Body. The individual identified for the task will be responsible for the management and enforcement of this policy.

5.1 Competent authority as identified by each Department/Ministry/Statutory Organization/Autonomous body
5.2 Designated nodal officer identified by each State/Ministry/Department
5.3 Implementing agency i.e. National Informatics Centre

6. Principle of Acceptable and Safe Usage

6.1 **General:**

IT resources provided by the Government are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other Government related purposes.

6.2 **Monitoring and Privacy:**

Users have limited right to privacy while using the Government's IT resources. The Government monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files under intimation to the user.. This includes any items stored on Government provided devices, such as files, e-mails, cookies, and Internet history. The Government reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials and authorized investigating agencies, as appropriate and consistent with applicable law.

6.3 **Use and Ownership**

Officials are responsible for exercising good judgment regarding the reasonableness of personal use. Individual organisations are responsible for ensuring adoption of this policy. If there is any uncertainty, employees should consult the competent authority of that respective site.

6.3.1 Any information that users consider sensitive or vulnerable should be encrypted.

6.3.2 For security and network maintenance purposes, authorized individuals from the implementing agency may monitor equipment, systems and network traffic at any time. Implementing agency reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6.3.3 Ministries/Departments/statutory bodies/autonomous bodies (henceforth referred to as "organisation") must establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

6.3.4 Competent authority of each site is responsible for implementing the requirements of this policy, or documenting non-compliance with this policy.

6.3.5 Competent authority of each organisation is required to train employees on policy and document issues with Policy compliance.

7. Security and Proprietary Information

7.1 Officials should take all necessary steps to prevent unauthorized access to their information.

7.2 Officials should keep their passwords secure and should not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed as per the password policy available on http://www.deity.gov.in/content/policiesguidelines under "Policy on Acceptable use of IT Resources".

7.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

7.4 Information contained on portable computers is especially vulnerable, hence, special care should be exercised. Refer point no 13

7.5 All hosts used by the official that are connected to the Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database and operating system patches.

7.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. For more details, please refer to the "Email Policy of Government of India".

7.7 Employees must report any loss of data or accessories to the competent authority of that respective organisation.

7.8 Employees should keep the system and sensitive data secure from outsiders.

7.9 Employees must obtain authorization before taking equipment outside an organisation.

7.10 UPS system with adequate battery backups must be installed to avoid any data loss or corruption due to power failure.

7.11 System should be properly shut down before leaving the office

7.12 Employees must follow instructions or procedures that come from the implementing agency/competent authority from time to time.

7.13 The users are responsible for maintaining the security of the Internet Service, including protection of account details, passwords and protection against unauthorized usage of their Service by a third party. The users shall be responsible for all charges incurred by other persons who they allow to use their Internet Service, including anyone to whom they have disclosed their password and account details.

7.14 If an officer wishes to use a Government service for instance Email service, from an external network, Use of VPN/OTP to access Government enabled services and resources is recommended.

8. System and Network Activities:

8.1 **Accessing private email servers from Government networks**: Officials must not access private e-mail servers from Government of India network. For all official correspondence, "Email service" authorized by the Government will only be used. For personal correspondence officer is allowed to use the personal email id assigned to him/her on the Government authorized Email Service.

8.2 **Using private email service providers for conveying official messages/documents**: Officials of Government of India under both Central and State Government shall not use the service of any other email service provider other than the one offered by Government of India. Refer to "Email Policy of Government of India" for the same.

8.3 **Accessing social media sites from Government owned systems**

8.3.1 Officers need to understand that Information once posted to a social networking site, is no longer private. The more information an official posts, the more vulnerable he/she may become. Even when using high security settings, friends or websites may inadvertently leak his/her information.

8.3.2 Personal information shared by an officer could be used to conduct attacks against his/her department.

8.3.3 Information gleaned from social networking sites may be used to design a specific attack against a particular department.

8.3.4 Although access to a social networking site can be detrimental to the functioning of certain aspects in the Government framework, Government recognizes that an officer may wish to use social media in his/her personal life. Hence, the use of a social networking site from a Government network is governed by the following to ensure that the risk of any damage is minimized:

8.3.4.1 Officers shall not identify him/her as a public servant. The officer is personally responsible for the content he/she publishes in a personal capacity on any form of social media platform.

8.3.4.2 Officer shall comply with all relevant points mentioned in the IT Act.;

8.3.4.3 Officer must adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and the department's Personal Information Policy.

8.3.4.4 IRC is one of the most common means of sharing information. Officers shall not click on a link shared during an IRC as it can lead to downloading of malicious code on a Government access device (desktop/laptop etc).

8.3.4.5 Officer must report suspicious incidents as soon as possible.

8.3.4.6 Officer must always use high security settings on social networking sites, and be very limited in the personal information you share.

8.3.4.7 Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated.

8.3.4.8 Officer must not post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, or is otherwise unlawful;

8.3.4.9 Officer must not imply that he is authorised to speak as a representative of the department or the government, nor give the impression that the views you express are those of the department or the government;

8.3.4.10 Officer must not use his department email address or any department or Government logos or insignia that may give the impression of official support or endorsement of your personal comment;

8.3.4.11 Officer must not use or disclose any confidential information obtained in your capacity as an employee/contractor of the department;

8.3.4.12 Officer must not make any comment or post any material that might otherwise cause damage to the department's reputation or bring it into disrepute.

8.3.4.13 Users should also refer to the "Framework and Guidelines for Use of Social Media for Government Organisations" available on http://deity.gov.in.

8.4 **Misuse of a service**: The user is responsible for his/her actions on the network of the implementing agency and the devices assigned to him/her by the Government. Any irresponsible action by the user which endangers the security of the network or compromises systems or equipment would result in termination of his/her network service without prior notice.

8.5 **Sharing of data**: Officials must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.

8.6 **Use of personal email id**: User must not use their personal e-mail ID for purposes of official communications. Refer the "Email Policy of Government of India" for more details.

8.7 **Use of freeware software:**

8.7.1 Users should not copy or install any software on their own, including privately owned shareware, freeware or through CDs/DVDs without the approval of the competent authority.

8.7.2 Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of a computer resource.

8.7.3 If a user suspects that his computer has been infected with a virus (erratic or slow behaviour), the same should be reported to the system administrator for corrective action.

8.8 **Filtering and blocking of sites**:

The Government will block content over the Internet that the Government considers inappropriate. This includes pornography, obscene material, share and trading sites, games site, job sites, online shopping sites and other material that may hamper the working of the user. The Government may also block other content deemed to be inappropriate, lacking educational or work-related content or that pose a threat to the network. The Government may, in its discretion, disable such filtering for certain users for bona-fide research or other lawful educational or Government purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities.

9. Network Monitoring:

Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

9.1 Implementing agency may scan any IP address ranges allocated to an officer or an organisation in order to detect the presence of open or otherwise misconfigured mail and proxy servers. If a misconfiguration is detected in a proxy server/any device connected to the network implementing agency is authorized to take it off the network.

9.2 Officer shall not execute any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

9.3 Officer shall not Use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

9.4 All the devices the officer uses must be loaded with the appropriate anti-virus. If the officer takes the portable devices such as laptops / tabs etc. outside the premises (on tour etc.), he/she needs to get the device scanned for any kind malicious code /

Trojans etc. before connecting it to the network. Efforts will be made to carry out this process automatically while connecting it back to the network.

10. External Storage Media

10.1 Threats of using External Storage Media:

USB portable storage devices pose the following kinds of threats:

10.1.1 They allow users to bypass perimeter defences, including firewalls and email server antimalware, and potentially introduce malware into the office. Since the malware enters the network from an internal device, it may go undetected until significant damage is caused to the network.

10.1.2 Portable storage devices allow employees, social engineers, and intruders in general to remove sensitive information from an organization's premises. This information might include protected classified information.

10.1.3 The impact of an information compromise by either of these threats, including the accidental loss of information through the loss of a device, could impact the Government service framework.

10.2 Use of External Storage Media:

10.2.1 Based on the above, use of external storage, by default will not be allowed in the Government framework. If an officer needs to use the same in line with his work, due approval from the competent authority of that respective organisation needs to be taken. If use of an external storage media is not part of the functional requirement of an officer, the same will not be issued. Blocking access to external storage on a Government issued access device like desktop/laptop etc needs to be done by deploying “end-point-compliance” at all organisations in the Government framework. Officers who use the external storage after due approval need to adhere to the following:

10.2.1 Officer shall use the media issued by the department only. The official is responsible for the safe custody of devices and contents stored in the devices which are in their possession.

10.2.2 The official should store classified data in a separate USB memory device and it should not be shared. Non-Classified data may be stored on a different USB memory device.

10.2.3 The classified data should be encrypted before copying into the USB device designated to store classified information. The key to decrypt files should not exist on the same device where encryption data exists.

10.2.4 For Top Secret information separate portable media should be used.

10.2.5 Unused data on USB devices shall be wiped using multiple pass process (like wipe/eraser software).

10.2.6 Officers should not allow USB device belonging to outsiders to be mounted on Government systems.

10.2.7 The officer should scan the USB device, which was used on any outside system including the PC at home for any virus before copying any data on the official system.

10.2.8 The modification of documents of USB drive should be carried out without copying into the target system.

10.2.9 The individual should return the USB devices issued to him upon transfer or retirement.

10.2.10 In case of damage or malfunction of device, the same shall be returned to the concerned official for issue of a substitute.

10.3 **Use of External storage media by a visitor**: Visitors to an organisation are not allowed to carry any potable media without permission. If it is necessary to allow the visitor to use USB memory device for any reason, it should be used only on designated systems meant for presentation purpose in the office. Under no circumstances the USB device belonging to visitors should be mounted on systems that are connected and belong to the Government framework.

10.4 **External storage devices issuing authority of each organisation shall adhere to the following:**

10.4.1 A record shall be maintained for procurement, issue, return, movement, destruction of the portable devices.

10.4.2 If necessary the department may issue two types of devices which are easily distinguishable in shape, colour and make. Individuals may be given instructions, which one of the two will be used for classified data.

10.4.3 The USB memory device used for storing classified data should have a password protect mechanism for read, write, delete.

10.4.4 All obsolete USB devices shall be physically destroyed.

10.4.5 A verification of USB devices should be carried out by issuing authority at regular intervals of 3 months by way of self certification by individuals that the pen drives issued to them are under their safe custody.

11. Preventing spread of malicious software

Material downloaded or received over public networks may contain viruses or other malware. When it is necessary to download files, officer should only do so from known or trusted sources. Officers should show extreme caution when opening email attachments, particularly if they have been sent to them by someone they do not know, or if the sender seems suspicious. A computer may also be infected by software loaded from websites, either intentionally or accidentally. Users should be careful not to download any software from such sites and follow the following best practice:

11.1 **Best Practice:**

11.1.1 Do not open emails from dubious sources;

11.1.2 Do not reply to Spam or click on links, including 'unsubscribe' facilities, in Spam;

11.1.3 Do not post your email address on publicly available sites or directories. If you must do so, look for options, such as tick boxes, that allow you to opt out of receiving further offers or information.;

11.1.4 Do not disclose your personal information to any online organisation.

11.1.5 Ensure that web reputation filter is enabled in the antivirus software installed.

11.1.6 For more details regarding the above, refer to the "Security Policy" for a user available on http://www.deity.gov.in/content/policiesguidelines under "Policy on Acceptable use of IT Resources" and "E-mail Policy of Government of India" available on http://www.deity.gov.in/content/policiesguidelines under "E-mail Policy".

12. Security Incident Management Process

12.1 An incident response and management is necessary for detecting security incidents, minimizing loss and damage, mitigating the weaknesses that were exploited and restoring information assets in a timely manner.

12.2 This process is applicable to all policy violations reported by the Administrator or the Users.

12.3 The implementing agency reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of the framework

12.4 Any such incident must immediately be brought to the notice of the CERT-In and the implementing agency.

13. Use of Portable Devices

13.1 Mobile and portable computing devices are devices such as tablets, smart phones, and laptop computers. The very features that make these devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to Government of India when they contain important Government data. The following best practices should be followed by all users:

13.2 General Security

13.2.1 Users should keep their mobile devices with them at all times or store them in a secured location when not in use. They should not leave their mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

13.2.2 Mobile and portable devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is enabled. The password used should be as strong a password as the device will support.

13.2.3 Enable a “remote wipe” feature if available. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.

13.2.4 Users should not circumvent security features or otherwise “jailbreak” their mobile device.

13.2.5 Standard security protocols should be followed. This includes ensuring that the device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.

13.2.6 Users should Wipe or securely delete data from the mobile device before they dispose of it.

13.2.7 Lost, stolen, or misplaced mobile devices should be immediately reported to the security Incident team (refer point no 12 above).

13.3 Transmission Security

13.3.1 Where possible, data transmissions from mobile devices should be encrypted.

13.3.2 Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.

13.3.3 Available wireless access should be configured to query the user for confirmation before connecting to wireless network

13.3.4 Users should be careful when using insecure networks and should use VPN services to connect to Government resources. Most modern mobile devices are supported with proper configuration.

13.4 Application and Data Security

13.4.1 Do not install software from unknown sources as they may include software harmful to the device. Research the software that you intend to install to make sure that it is legitimate.

13.4.2 When installing software, review the application permissions. Latest applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.

13.4.3 Be careful when storing the personal data on the mobile device.

14 Intellectual Property

14.1 Material accessible through the implementing agency's Network 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 Network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

15 Enforcement

15.1 This **"Policy on Acceptable Use of IT Resources"** is applicable to all employees of Central and State Governments. It is mandatory for all users to adhere to the guidelines of the policy without exception

16 Suspension or Termination

16.1 The implementing agency reserves the right to suspend a resource to the user if he/she is in breach of this Policy. It will first take reasonable steps to contact the user and give him the opportunity to rectify the breach within a reasonable period. What is reasonable in this context will depend on the severity of the problems being caused by the breach

17 Exception Management

17.1 For any special permission/exception, the user shall take approval from the competent Authority of his respective Organisation. The request will be routed through the implementing agency subsequent to approval from Competent Authority.

18 Review

18.1 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:

18.1.1 Impact on the risk profile due to, but not limited to, the changes in the deployed technology/, regulatory and /or legal requirement.

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

GLOSSARY

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Organisation	Ministry/Department/Statutory Body/Autonomous body under Central and State Government
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Security Incident	Any adverse event which occurs on any part of the Government service framework and results in downtime/breach of the framework.
System Administrator	Officer responsible for administering the IT systems and applications
Nodal Officer	Officer responsible for all matters relating to this policy who will be coordinating on behalf of the Organisation
Competent Authority	Officer responsible for taking and approving all decisions relating to this policy in his Organisation
Implementing Agency	National Informatics Centre. A Body which will be responsible for ensuring compliance to this policy including power to impose penal measures.
Users	Refers to officers/personnel who are accessing the Government services
Social Media	Applies to social networking sites, blogs, electronic newsletters, online forums, social networking sites, and other services that permit users to share information with others in a contemporaneous manner.
External Storage	**External storage** is storage that is not part of the computer. e.g. pen drives
IRC	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat) or synchronous conferencing It is mainly designed for group communication in discussion forums, but also allows one-to-one communication via private message] as well as chat and data transfer,

Secret

Copy no…….

F.no. 10(4)/2011-EG-II(Part File)

Ministry of Communication & Information Technology

Department of Electronics & Information Technology

Date: Oct 2013

NOTE FOR THE COMMITTEE OF SECRETARIES

Subject: "Email Policy of Government of India" and "Policy on Acceptable Use of IT Resources of Government of India" - Drafts for approval

A. Email Policy of Government of India

Back ground

Email service is a major mode of communication in Government of India. Communications include Government information and data that travel as part of e-mails amongst the users throughout the country or anywhere in the world. e-mail services form the critical component of e-Governance framework, and as a back end tool, they enrich the e-governance applications to offer enhanced services.

2. e-mail messages contain sensitive and often confidential information. Given the current cyber security scenario, Government emails are a prime target for cyber attacks. It is, therefore, vital that high levels of security be used for email, both at storage and in transit. These days, most of the malicious programs (viruses, trojans and worms) are spread through email message attachments. Hence, it is important to ensure that email messages are safe even when stored, so that confidential & sensitive information is not leaked out of Government departments.

3. Realising the growing importance of e-mail services in Government communications, it is proposed to formulate an e-mail Policy for Government of

India. As per the proposed policy, email accounts will be given to all the employees of the Central Government and to the employees of those State Government, which are already using the NIC's e-mail services and it will be mandatory for all employees to use this email service. The use of email accounts of private e- mail service providers like will be prohibited for official communication.

4. For creating and operating this ecosystem in the Government, a draft "Email Policy of Government of India" has been prepared by DeitY (enclosed as annexure 'A'). This policy of the Government of India (GoI) lays down the guidelines with respect to use of email services. The implementing agency for this service shall be National Informatics Centre (NIC), under the Department of Electronics and Information Technology, Ministry of Communications and Information Technology.

Objective of the Policy

5. The objective of this policy is to ensure secure access and usage of GoI email services by its users. Users have the responsibility to use this service in an efficient, effective, ethical and lawful manner. Use of the GoI email service amounts to the user's agreement to be governed by this policy. This policy proposes to cover all employees of Central Government and the employees of those State Governments, which are already using the NIC's e-mail services, and other State Governments which adopt these services in future.

Main Policy Measures Proposed

6. The main policy measures proposed are as follows:-

i) As there are significant security concerns associated with the use of email services provided by external service providers, it is proposed that NIC will

be the only email service provider for Central and State Governments. Choosing to adopt this policy.

ii) All existing email services, other than the GoI email service, if any, being used in any Government organization should be migrated to the GoI centralized email service in a time bound manner.

iii) Mandatory use of Digital signatures (DSC) is prescribed for transmission of classified, confidential or restricted data by email. Wherever considered necessary, classified information shall be transmitted using encryption.

iv) Use of Static IP addresses/Virtual Private Networks(VPN)/One Time Password(OTP) for accessing the GoI email services by Government of India officials stationed at Embassies or working in Missions or on deputation abroad is stipulated.

v) The stipulation at (iv) above whall be applicable to the employees of GOI and of the State using NIC's mail services, when they are on tour abroad.

Key Aspects of the policy

7. The Key aspects covered in the proposed policy are as below-:

i) Security of emails and data in the documents attached thereto, authentication of sender of an email for officials stationed outside India, prohibition of using other mail service providers for official mails, deactivating/resetting of passwords by implementing agency in case of compromised email ids;

ii) Best practices like frequent change of passwords, not saving passwords, verifying SSL(Secure Socket layer) certificates before accepting, logging out from mail accounts when idle, use of only official portable storage

media, use of digital signature for sending an email containing any sensitive information;

iii) Process of creating email accounts after authorization by competent authority, providing virtual domains, delegating admin console service to organizations/ministries/departments for their respective domain, deactivation of mail account based on designation before leaving an organization on transfer;

iv) Confidentiality of email messages and guidelines for using strong and secure passwords;

v) Scrutiny of emails/release of logs to ICERT, NTRO or any other GoI authorized agency under exceptional circumstances relating to national security, abuse incidents or violations of other policies;

vi) Policy for data backup and data retention for email data;

vii) Policy for deactivation of email accounts in case of resignation, superannuation;

viii) Roles and responsibilities of users and respective organizations as related to email accounts;

ix) Guidelines for dissemination of this policy and its enforcement.

B. Policy on Acceptable Use of IT Resources of Government of India

Background

8. Government of India provides Information Technology (IT) resources and the services accessible on them to all its employees, permanent or contractual, and other authorized workers across various Ministries/ Departments/ Statutory Bodies/

Autonomous Bodies under both central and state Governments. These resources and services help a Government official perform his/her duties efficiently.

9. However, any misuse and abuse of these resources can offset the advantages and may result in unwanted risk & liability for the Government. To address this issue, it is proposed to formulate a "Policy on Acceptable Use of IT Resources of Government of India.

10. For creating and operating this ecosystem in the Government, a draft "Policy on Acceptable Use of IT Resources of Government of India" has been prepared by DeitY with clear role definitions (enclosed as Annexure-B). This policy of the Government of India lays down the guidelines with respect to use of all IT resources. This policy shall apply to all employees, contractors, consultants, temporaries, and other workers of Government of India, including all personnel affiliated with third parties. This applies to all IT resources, owned or leased by Government of India, and services accessible on them.

Objective of the policy

11. The objective of this policy is to ensure proper access and usage of Government of India IT resources by its users. Users have the responsibility to use these resources in an efficient, effective, ethical and lawful manner. Use of the IT resources offered by Government of India amounts to the user's agreement to be governed by this policy. For the purpose of this policy, the term "IT resources" includes:

- Computers and desktop devices
- Portable devices such as laptops, PDAs, tablets and mobiles
- External storage devices such as Pen Drives

- Personally-owned devices connected to GoI resources and
- Network resources such as internet connections, email accounts, etc.

Key Aspects of the Policy

12. The key aspects covered in the proposed policy are as below-:

i) "Security and Proprietary Information" guides the users about necessary steps to be taken to prevent unauthorized access to their information. This includes keeping their systems and sensitive data secure with passwords, updating their systems with approved virus-scanning software and patches, using extreme caution while opening email attachments,etc.

ii) "System and Network Activities" advises against accessing private email servers from Government networks, using private email service providers for conveying official messages/documents, accessing social media sites from Government owned systems, sharing of data, use of freeware software unless specifically permitted etc.

iii) "Network Monitoring" addresses issues relating to security breaches through users logging into servers or accounts that they are not authorized to, using any form of network monitoring to intercept data not intended for them or using any program/script/command with the intent to interfere with other user's terminal session.

iv) "External Storage Media" provides guidelines for users and issuing authorities about use/issue of pen drives, external hard discs ,etc..

v) Preventing the spread of malicious software like materials downloaded or received over public networks containing viruses or other malware by

following the best practices like not replying to spam, not clicking on links, not disclosing personal information to any online portals etc.

vi) Use of portable devices, their general security, transmission security, and application & data security.

vii) Security incidence and management process for detecting such incidents, minimizing loss and damage, mitigating the weaknesses that were exploited and restoring information assets in a timely manner.

viii) Guidelines for enforcement, suspension or termination and exception management.

13. The draft Note was circulated to various Ministries/Departments of GoI and all State Government . The comments of these Ministries/Departments/State Government are enclosed as Annexure-C (to be added).

14. Decision of COS is sought on the above mentioned policies enclosed as Annexure-A & Annexure-B.