<u>Review Comments on "E-Mail Policy and Policy on Acceptable Use of IT Resources of GoI"</u>

As per the discussion held in the office Chamber of Director (IT) on 30<u>th</u> and 31<u>st</u> October, 2013 in which following members were present:

  i. Sh. Rajeev Sharma (Joint Director, DIT,HP)
  ii. Sh. Anil Semwal (Deputy Director, DIT,HP)
  iii. Sh. Chaturbhuj Mishra (Principal Consultant-SeMT, DIT,HP)
  iv. Ah. Amit Kumar Agrawal (Sr. Consultant-SeMT, DIT,HP)
  v. Sh. Rakesh Verma (Project Manager, UID project,Accenture)
  vi. Sh Amit Singh (Software Designer, UID project,Accenture)
  vii. Sh. Kuldeep Singh Thakur (Consultant, KPMG)
  viii. Ah. Amit Kumar Singh (Consultant, e-District Project, Wipro)

Following Documents received from Deity, GoI for review and feedback:

  i. Email Policy of GoI
  ii. Policy on Acceptable Use of IT Resources of GoI

Comments/Suggestions on Email Policy

S.No.	Reference	Comments/Suggestions
1.	General Comments	It is suggested that NIC mail should have following value added services to increase productivity of employees/users: i. Mail Forwarding ii. Calendar Sharing iii. Calendar Import and synchronization with Google Calendar (Two way synchronization) iv. Availability IMAP(Internet Messaged Access Protocol) protocol services v. To setup mail on any device such as Mobile phones, Tablets etc. auto configuration should be available from NIC mail server similar to GMAIL and Yahoo vi. NIC e-Mail client should work in all the major available browsers. vii. Rights to create groups should be provided to Nodal Officer viii. Unlike other mail services provider, the NIC mail is should also be user friendly, e.g. for storage of email addresses for purposes of auto fill etc.
2.	2.2 This policy is applicable to the	In Himachal Pradesh State, there are legal bodies

	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.	such as e-Governance societies where people are hired on contract basis and not State Government employees and these contractual people are working on various jobs assigned by different Departments therefore official e-mail is required for these contractual peoples. Furthermore Himachal Pradesh is in process to implement e-Office in various Government Departments and to use e-Office application having NIC e-mail is mandatory requirement. Therefore it is recommended that provision for e-mail creation for these contractual workers should be there in this e-mail policy.
3.	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.	Clarification required on this clause, is there any charge for using e-Mail services by other legal bodies such as e-Governance societies and other legal bodies (boards etc.) are not drawing their fund from the consolidated fund of India.
4.	3.3 This Policy supersedes any other E-Mail policy previously issued.	**Contradiction point:** In clause 3.2 it is mentioned that "Refer —NIC e-mail Services and Usage Policy available on http://www.deity.gov.in/content/policiesguidelines/ under —E-mail Policy " and in this point just opposite. Furthermore there is no e-Mail policy is available on the mentioned link "http://www.deity.gov.in/content/policiesguidelines/ under —E-mail Policy "
5.	e-Mail Migration	Clarification is required on following: • E-Mail Migration from public e-mail servers: Presently Many State Government Departments are using public domain e-mails such as GMAIL, Yahoo, and Hotmail etc. as official e-mails. Now these e-mail needs to be migrated to NIC e-mail server. • E-Mail Migration from Government e-mail servers: Presently Department of Information Technology is having e-mail exchange servers and creating e-mail for state Government employees, now these mails also needs to be migrated from these current state Government servers to NIC servers. Is that possible whether above existing mails can be migrated from old mail servers to NIC mail Servers and Who will do this migration?
6.	4.1.5.8 In case of a situation when a	Clarification is required on "the implementing

	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).	agency" i.e. Name and responsibilities. Furthermore SMS may be send on RMP (Registered Mobile Phone) of the user.
7.	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.	It is recommended NIC e-mail should allow to send e-mails to outside the Government of India also as it is very much required while interacting to various private agencies who are working as consultants/contractors/service providers for a Departments.
8.	4.2.3 It is mandatory for users stationed at sensitive offices to use OTP [5] for secure authentication.	Clarification is required on following: • What are sensitive offices? • Mechanism through which OTP shall be provided to the users
9.	4.2.5 Users must logout from their mail accounts whenever they leave the computer unattended for a considerable period of time.	It is recommended that NIC e-mail should have auto logout feature after 15 minutes.
10.	4.2.8 The —save password and auto complete features of the browser should be disabled.	It is recommended there should be server side control which should not allow users to save password locally in browsers.
11.	4.2.9 The files downloaded from the Internet or accessed from the portable storage media should be scanned for malicious contents before use.	It is recommended there should be server side scanning for upload and download both.
12.	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.	It is experienced many times that existing mail server SSL certificates gives errors in most of the browsers it is recommended it seamlessly.
13.	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	It is recommended there should be strong security controls at server side to prevent any security threats.

	DVDs.	
14.	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.	It is recommended there should be strong SPAM filter controls at server side to prevent any security threats.
15.	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 is changed. His successor will need to get the password reset once he takes over the post.	It is recommended that password reset request should be handled at DIO level at State itself to avoid any delay. Furthermore while resetting the password it should not check the previous passwords.
16.	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.	This clause it not acceptable as nodal officers in the State is not technical person, So it is recommended to remove this clause.
17.	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	It is recommended that this activity may be done centrally by organization/nodal officer instead by individual user.
18.	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.	Clarification is required on "implementing agency" and "other agency".
19.	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	IT is recommended to increase the period 30 days for Probably Spam i.e. Probably Spam (unsolicited e-mails) – 7 days (unsolicited e-mails) – 30 days
20.	4.12 Data Backup	IMAP should be enabled to increase the productivity of users.
21.	4.13.4 Inactive account: Any account which is inactive for a period of 90 days will be deactivated. The userid along	It is recommended to increase the period of 180 days to 360 days, furthermore inactivated mail id should be reserved for future use till 3 years. This feature is

	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 reopening of the said account with the same id, subject to availability. In such cases data from the backup will not be restored.	required as in case if official is on foreign assignment posting for long duration and when he/she join again then his earlier e-mail id is required.

Comments/Suggestions on "Policy on Acceptable Use of IT Resources":

S.No.	Reference	Comments/Suggestions
1.	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	It is recommended to include Consultants, Contractual employees working for State Government.
2.	3.5 Personally-owned devices connected to ACT Government resources and	Clarify what is the meaning of word "ACT".
3.	5.3 Implementing agency i.e. National Informatics Centre	Clarification is required in case of States, How NIC will be the implementing agency, in case if NIC will be the implementing agency then also specify the roles and responsibilities also.
4.	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.	It is recommended that all the users should be in the centrally controlled environment i.e. within the domain control.
5.	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.	In this clause "system administrator" roles needs to be clarified.
6.	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	More Clarification is required as in Himachal Pradesh there are two networks one is HIMSWAN and other is NIC network, it will be very difficult to implement these recommendations in HIMSWAN network because every user device connected with this network is not on the domain.

	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.	
7.	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.	It is recommended to relax this clause as many senior employee are using mobile devices and deletion of data will lead to so many problems.

****End of Document*****