



EMAIL POLICY

Author		Document name		Date of first issue	
Owner	C & IT Department	Document ref. no.		Date of latest re-issue	
Version	1.1	Page	1 of 7	Date of next review	
Issue Status	Under Review/ Live	Security classification	Internal use only	Reviewer	



EMAIL POLICY

VERSION CONTROL

Revision no.	Date of issue	Prepared by	Reviewed by	Approved by	Issued by	Remarks

DRAFT

EMAIL POLICY

OBJECTIVE

The objective of this policy is to define acceptable usage of Email services provided by NMDC.

SCOPE

This policy is applicable to all **Mail Administrator** and users of NMDC email and internet services.

POLICY RULES

IT System Management policy

1. Deployment of identity control of people for opening email account: All junior officers and executives shall be allotted with an email account. It will be opened with a default password that will be communicated to the user. The user has to change the default password in line with NMDC's Password Policy while logging in for the first time. All official communication shall be through this email account.
2. All users shall configure MS-Outlook on their laptops so that mails can be seen in offline mode also. Use of clients other than specified by company is not permitted.
3. All user are provided with the mailbox size set to 4 GB (2 GB + 2 GB) respectively.

Email Quota assigned: Email quota has been allocated as dynamic allocation with maximum cap, known as thin provisioning in which user mail box can grow upto maximum allocated quota size. If user is using less quota, balance allocated space can be shared among other users.

CMD/ Directors → 5 GB

RED/ED/HOP/GGM → 2 GB

GM → 1 GB

All Executives of XYZ Dept. → 10 GB

(Whenever executives will be transferred out from XYZ Dept., 10GB quota will be revoked & quota will be assigned as per level)

Marketing consultancy → 2 GB

All other users of XYZ Sites etc. → 500 MB

4. **De-activation:** Email ID of separated employee (superannuation, resignation, death etc.) should be immediately deactivated by Mail Administrator once information is received from Personnel Department. Any email to de-activated accounts should receive automatic reply with information about successor's/RO1's email id (to be received from concerned department) if required. Mail administrator would be given access to deactivated email ID for a period of 30 days. The account, mailbox and all the information should be deleted after this period.
5. **Disclaimer policy:** All outgoing emails from NMDC domain to other domains contain disclaimer message auto stamping.
"PLEASE DON'T PRINT THIS E-MAIL UNLESS YOU REALLY NEED TO."
DISCALIMER: This message (including any attachments) contains PRIVILEGED AND CONFIDENTIAL INFORMATION and is intended to be conveyed only to the designated recipient(s). If you are not an intended recipient, please notify the sender and the administrator at mailadmin@nmdc.co.in

Commented [BA1]: Department to specifically check all highlighted portions

Commented [BA2]: Department to provide input

EMAIL POLICY

immediately and then delete this message from your system. You must not copy, use, disclose, disseminate, distribute, or reproduce this message or any part thereof in any form. Any statement or information contained in this message not of an official nature shall not be deemed to be given or endorsed by NMDC Limited, or its relevant representative offices unless otherwise indicated by an authorized representative independent of this message. Risks are inherent in all Internet communication. While steps may have been taken to try to eliminate viruses and other harmful code or device from this message and its attachment(s) (if any), the sender is not responsible, and hereby disclaims all liabilities arising from or in relation to any viruses and/or other harmful code and/or device. Each recipient is responsible for protecting its system from viruses and/or other harmful code and/or device. NMDC reserves the right to monitor and review the content of all messages sent to or from this e-mail address. Messages sent to or from this e-mail address may be stored on the NMDC e-mail system.

NMDC Limited** End of Disclaimer"

6. Emails from NMDC domain exchanged with internet domains should be subject to necessary Antispam and Antivirus checks with suitable technology controls. Mail Administrator and/or any nominee of IT Security Nodal Officer will be authorized for monitoring of email for the above reasons. Unless specifically delegated, the task of monitoring email messages is prohibited for all other employees.
7. IT Security Nodal Officer for region with the help of Mail Administrator must establish and maintain a systematic process and standard for recording, retaining, archiving and destroying email messages and relevant accompanying logs. Destruction of logs and referenced email messages must be postponed whenever a legal notice is received.
8. Account lockout policy:-
 - Number of consecutive failed logins allowed: 5
 - Time window in which the failed logins must occur to lock the account: 1 Hour
 - Time to auto unlock the account: 1 Hour
9. Group Mail Privilege:
 - Site Group Mails (all employees of that site) → Head of project
 - Global Group (all employees of NMDC) → Head IT, Head of Corporate Communications, Head P&A
 - Local Group (as per requirement) → Any employee can send
10. Attachment

All local/in/out emails -Max message size with attachment → 30 MB

Attachment Type Blocked (Email will be quarantined)→ *.ade;*.cmd;*.eml;*.ins;*.mdb;*.mst;*.reg;*.url;*.wsf;*.adp;*.com;*.exe;*.isp;*.mde;*.pcd;*.scr;*.vb;*.wsh;*.bas;*.cpl;*.hlp;*.js;*.msc;*.pif;*.sct;*.vbe;*.bat;*.crt;*.hta;*.jse;*.msi;*.pl;*.scx;*.vbs;*.chm;*.dll;*.inf;*.lnk;*.msp;*.pot;*.shs;*.wsc;*.bmp;*.pcx;*.rtf;*.wav;*.mp3;*.midi;*.voc;*.mpeg;*.msvideo;*.quicktime;*.java byte code;*.rar;*.arj;*.tar;*.gz

(Attachment will be blocked for any other suspicious extensions detected in future)
11. Backup and Miscellaneous
 - Retention and journaling of emails sent/received outside NMDC shall be maintained with tamper proofing in the event of any traces to be made for emails transacted by any user (e.g. legal notice served to user).
 - Backup policy: Full backup will be done every Saturday in between 13:00 and 14:00

EMAIL POLICY

Incremental backups will be performed daily. (Daily backup will be transferred to Tape and will be removed from server after 2 days. Tape backup will be retained for 1 month before overwriting).

— Archive email policy: All inbound/outbound emails to/from NMDC (nmdc.co.in domain) will be archived for one year except internal emails.

Mail log retention/quarantine mail retention /quota warning/auto mail forwarder:

— Mail Log Retention Period → 60 days

— Logger Data Retention → 60 days

— Quarantine Mails Retention → 30 days

— Quota Warning Threshold Limit → 80% of mail box size

IMAP/SMTP/ POP Access → Access allowed from internet & internal LAN

Active Sync on mobile allowed with policy based security settings → all employees

Trash mail retention on server → 48 hrs

Maximum number of mail recipient allowed → 30

Users related policy

1. Users should keep their email credentials secure.
2. Email Client: Users must use only such clients which are identified by NMDC C&IT Department (at present this is **MS Outlook**) for accessing emails.
3. Users shall manage their mailbox in such a way that all unwanted/read mails are deleted on regular basis.
4. Auto archiving feature shall be kept enabled so as to manage the allocated Mail Box storage to user.
5. Users should be aware that email is vulnerable to unauthorized access and modification by third parties.
6. Email transmissions via internet generally consist of multipoint communications that are routed to their destination through the path of least resistance, which may include multiple foreign and Indian Internet service providers (ISP). It may be noted that any information when transmitted on Internet remains resident on an ISP server, until it is overwritten.
7. Unencrypted email transmissions are subject to a risk of compromise of information confidentiality or integrity.
8. Users must not use an "auto-forward" function to send emails to an address outside the company's network.
9. Users shall not use the Internet or email resources for any purposes, which conflicts with the interest of the company.
10. It is a violation of company policy to use the company email system for personal purposes.
11. Users must not register a company email account on an external mailing list for receipt of email (other than business purposes).
12. Users must not use distribution lists from the global addresses list for personal items of email.
13. Incidental personal use of email is permissible as long as it does not
 - Interfere with normal business activities of the company or hamper employee productivity
 - Consume more than trivial amount of resources
 - Involve solicitation
 - Associate with any outside business activity for personal gain

EMAIL POLICY

- Potentially embarrass the company and its management
- Include users requiring substantial expenditure of time
- Involve use for profit making
- Involve uses that would otherwise violate company policy with regard to employee time commitments
- Directly or indirectly interfere with the NMDC operation of computing facilities or electronic mail services

Users must specially label any personal email as such, or must send personal messages only by means that clearly identify the messages as personal in nature. Any messages sent without such labeling or identification may be assumed by the company to have been sent on behalf of the company (for whom the users will ultimately be held responsible).

14. Users should avoid using their personal email address as contact addresses for conducting company business operations.
15. Users should not forward business sensitive emails originating from either NMDC or from Customer domains, Joint Ventures or Partners to any free public email domains such as BUT NOT LIMITED TO Yahoo, Hotmail, Rediff mail, Gmail, etc.
16. Users shall not reveal or publicize confidential or proprietary information, but is not limited to financial information, new business and product ideas, strategies and plans, databases and information contained therein , technical product specification information, evaluation, s/w source codes, computer network resources, access and business relationships.
17. Users should not use their email and internet services for any unauthorized purpose targeting company, colleagues and other general public for areas, such as but not limited to:
 - Use of the resources in connection with surveys, contests, chain letters, junk email, spamming, or any duplicative or unsolicited messages
 - Defame abuse, harass, stalk, threaten or otherwise violate the legal and privacy rights.
 - Publish, distribute, or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful material.
 - Knowingly transmit, upload or download any material that potentially contains viruses, Trojan horses, worms, time bombs or any other harmful or deleterious programs.
 - Forward or send messages that have racial or sexual slur, political or religious solicitations, or any other messages that are inappropriate and/or has the potential to cause NMDC, harm or embarrassment.
18. Users should actively disclaim speaking for NMDC unless they have authority to do so. Note that if NMDC email system is used to post an article/message, NMDC's name is carried with what is posted. The "standardized" disclaimers attached to many articles are meaningless if the reader finds the article offensive.
19. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of NMDC or any unit of NMDC unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing NMDC. An appropriate disclaimer is: "These statements are my own, not those of NMDC"

EMAIL POLICY

20. Email attachments: Users must not open attachments that are from unknown or untrusted sources. While sending emails with attachments, users should attach compressed files.
21. Users must regularly move important information from email message files to word processing documents, text files and other files.
22. Users should not employ a scanned version of his/her signature to give the impression that the sender signed the message or other electronic communication, as another person could misuse the signature.
23. Internal email should be used for electronic approvals and valid documentary evidence.
24. Management has rights to review email content: All messages sent by users of company email account are company records. At any time and without prior notice, the management reserves the right to examine email, personal file directories or any other information stored on user devices. Email messages may be monitored for any reasons which could be, but not limited to;
 - Ensuring internal policy compliance
 - To support internal investigations for suspected criminal activity
 - To assist in the management of information systems of company
25. NMDC reserves the right to disclose email messages sent or received to law enforcement officials without prior notice to the employees. Users must restrict their communication to business matters in recognition of this electronic monitoring.
26. The distribution of any information through the internet, computer based services, email/ messaging system, is subject to scrutiny by NMDC. The organization reserves the right to determine the suitability of this information and monitor usage for unusual activity.
27. Users should acknowledge that their misuse of the resources may result in the breach of confidentiality with relation to NMDC or third parties, and they should adhere to all confidentiality and restriction of publicity obligations they are bound by with NMDC and to third parties.
28. Violations of these terms governing the use of the resources, with or without intention, will result in breach of policy and restriction of access to the resources and may include actions which requires an investigation and appropriate disciplinary action to be taken, up to and including termination from services.
29. Users are encouraged to report breaches of this policy to their supervisor or an appropriate senior officer or executive.
30. Internet and email use should be consistent with the NMDC's code of conduct, and Information Technology Act 2000 (and amendments to it).
31. C&IT reserves the right to disable any email account if there is a breach or the mail id has been compromised.

Commented [BA3]: Department to determine who is authorized to request such actions