

General IT Security Guidelines for Office Desktops/PCs.



IndianOil

Version 1.0

1. Physical Security

- 1.1. There shall be owner for each PCs/workstations/computers and he/she shall be responsible for usage of same.
- 1.2. Physical Access to PCs/workstations/computers by unauthorized person shall be strictly prohibited.
- 1.3. All PCs/workstations/computers shall be switched off when not in use.
- 1.4. Internet connections through local modems, broadband, Data Card or any other external media/devices shall not be used.
- 1.5. USB and CD/DVD ROM access shall be disabled in PCs in Critical locations like S&D, Control Rooms at all locations.
- 1.6. Access to the Data center/Computer center/Server room shall be through Access control system.

2. Anti Virus/Network Security

- 2.1 All the PCs/workstations/computers shall be protected by Anti-virus Software/Endpoint Protection Software and the same must not be disabled at any time.
- 2.2 It shall be the responsibility of the user to check all removable and portable media for virus before they are used within the Corporation.
- 2.3 Anti-virus software on all workstation and window based server shall be regularly updated with the latest anti-virus patches through automated process or by the IS Department representative.
- 2.4 No storage media brought in from outside the Corporation shall be used until it has been scanned.
- 2.5 New customized software shall be scanned for viruses before it is installed.
- 2.6 In the event of a possible virus infection the user must inform the IS Department immediately. The IS Department shall then scan the infected machine, any removable media or other workstations to which the virus may have spread and eradicate it.



IndianOil 3. OS and Application Level Security

- 3.1. User Name and Password for PCs/workstations/computers, SAP and other password protected applications shall not be shared with anyone at any cost.
- 3.2. User must logout when they leave their table/workstation/computer for any length of time. PCs/workstations/computers shall be set to get locked after idle time of 5 minutes.
- 3.3. SAP is configured to logout after 15 minutes of idle time. However, user shall log out of SAP every time they leave the PC unattended even for short durations.
- 3.4. Users shall not install any software on their computers without approval of the respective IS department.
- 3.5. IS Department shall ensure that Administrator password of the PCs/workstations/computers/servers shall not be kept blank.
- 3.6. PCs/workstations/computers in critical locations like S&D shall only have SAP Client, Lotus Notes/MS Outlook, MS Office and other approved software.

4. General Guidelines

- 4.1. Use of Wireless devices including data cards and Bluetooth shall be strictly prohibited to be connected to PC on LAN for local network/internet access.
- 4.2. Internet and other external service access shall be restricted to authorised personnel only.
- 4.3. Access to data on all laptop and computers shall be secured through boot password, to provide confidentiality of data in the event of loss or theft of equipment.
- 4.4. The use of unauthorised software is strictly prohibited.
- 4.5. Access to workstation shall be user based. User accounts shall be managed through Active Directory (AD).
- 4.6. All demonstrations by vendors shall be run on vendor's machines only.
- 4.7. Users shall be aware of and adhere to Corporation's Policy on Internet, e-mail and pen drive Usage.

4.8. Users shall give permissions only to the authorized users to access the shared files from their computers through AD.

5. Internet and e-mail usage Policy

5.1 User access to Internet, e-mail and USB pen drive/Flash drive shall be governed by the Policy given in **Annexure – A**.

6. General Guidelines for Choosing a Secure Password

In order to make it harder for people to guess passwords please keep in mind the following advice:-

- a) Don't use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, *etc*.
- b) The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first thing potential crackers will try when guessing your passwords.
- c) Instead try to pick acronyms, mnemonics, random letters, *etc*, or insert non-alphabetic characters in the middle of the word, replace letters with numbers ('o' to zero, l to 1, E to 3), *etc*.
- d) Do include a number (0-9) somewhere in the password.
- e) Never tell anyone else your password or allow them to log in as you. Avoid telling anyone password on the telephone. If it is necessary to provide password to someone else to allow a fault to be fixed, ensure that they are genuine members of Information Systems Department and then change the password.
- f) Try to avoid letting other people watch while entering password .

Internet Usage Policy

1.0 Statement of Policy

Use of the internet by employees of Indian Oil Corporation Ltd. (IOCL) is permitted and encouraged where such use supports the goals and objectives of the business.

The internet access Permission and e-mail usage is guided by IOM ref. DP/7/4 dt. 29.10.2004 from ED (HR), CO enclosed.

This Policy will be reviewed from time to time by the empowered committee.

2.0 Scope of this Policy

- 2.1 It applies to everyone using the Internet in the Corporation. It includes all employees, contractors, supervisors, and students etc.

3.0 Definitions

- 3.1 Internet Usage includes, but not limited to, the following:
- a. Email
 - b. Accessing Web Sites
 - c. Accessing News Group
 - d. Chat
 - e. Files sharing/upload/download
 - f. Telnet

4.0 Internet Usage

4.1 Business Use

All Internet and computer usages are meant for business purposes only. Internet usage is a privilege reserved for those with a business need.

5.0 Monitoring Internet Usage

- 5.1 At any time and without notice, the Corporation maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems.

- 5.2 Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the Corporation. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.
- 5.3 In order to ensure compliance with this policy, the Corporation may employ monitoring software to check on the use of the internet and logs thus generated can be used for Disciplinary Action as defined in Section 9.0 below.
- 5.4 The Corporation can and will use blocking software to block access to websites that are considered detrimental to the performance of Corporation's Information Technology assets.
- 5.5 The Corporation can and will block certain Internet activities that are deemed unsuitable and/or unacceptable.
- 5.6 The Corporation specifically reserves the right for authorized personnel to access, retrieve, read and delete any information that is created by, received or sent as a result of using the internet, to assure compliance with all policies.
- 5.7 Such monitoring will be used for legitimate purposes only by the Corporation or Corporation's authorized representatives.

6.0 Activities not permitted

- 6.1 In particular the following activities are deemed unproductive by the Corporation and therefore NOT permitted:
 - a. Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material & downloading the same.
 - b. Using the computer to perpetrate any form of fraud, or software, film or music piracy.
 - c. Using the internet to send offensive or harassing material to other users.
 - d. Downloading of music/video, playing music/video.
 - e. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license.
 - f. Access into unauthorized areas.
 - g. Publishing defamatory and/or knowingly false material about the corporation, colleagues and/or customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
 - h. Undertaking deliberate activities that waste employees effort or networked resources.
 - i. Introducing any form of malicious software into the corporate network.
 - j. Users should not access/upload/download materials that can be deemed objectionable to other employees.
 - k. Any other action that is prohibited by law/ corporation policies/IT Act.



IndianOil

- 6.2 No desktops/Laptops/Mobiles in any LAN will be permitted to be connected to the Internet through attachment of any modem (Broadband / LL / Cable / PSTN), or Data card etc.

7.0 Confidential/Sensitive Material

- 7.1 Users should not upload/save/send Corporation's confidential and/or sensitive material to the public or any locations.

8.0 Misconduct

- 8.1 Where it is believed that an employee has failed to comply with this policy, he/she will face the disciplinary action as per Corporation's Policy.



IndianOil



CORPORATE HRD

Inter Office Memo

File Ref: DP/7/4

Date: Oct 29th, 2004

From: ED (HR)

To: ED (HR), PL HO / ED (HR) Mktg HO / GM i/c (HR) RHQ / DGM (HR), R&D

Sub: Policy for usage of email & Internet

The following policy guidelines for use of email & Internet have been approved by the Management and may be followed by all the divisions.

IOCL provides various facilities to its employees for improving the productivity of the employee such as PCs, Laptop, Internet Access, e-mail etc. on need basis. It is necessary that these facilities are used judiciously and for official purposes only. This Internet usage policy has been designed keeping in mind enhanced PC penetration, the network security aspects and the need to avoid misuse/malicious use of Internet.

Policy for allowing Internet Access:

1. Officers having networked PC will normally be provided e-mail facility. However, internet access will be provided to officers in grades "A" to "E" on need basis, on specific recommendation by HOD/location in charge in grade "G" and above.
2. Non-officer employees shall be provided e-mail on their PCs for specific purposes as certified by the Head of the Department and after due approval of the designated Competent Authority. (Grade "H" and above)
3. E-mail account shall be closed immediately on the separation of the employee by way of Retirement, Resignation and Death etc.
 - 3a. Use of e-mail/Internet facilities is prohibited for malicious activities like downloading of music/video, playing music/ video, visiting pornographic sites & downloading pornographic pictures etc.
 - 3b. The server logs and the electronic 'paper trails' shall be considered proof for deciding misuse of e-mail and Internet.
4. The internal communication should be preferably done using the corporate mailing system. The Fax messaging should be used only when the e-mailing is not possible.
5. Only System Administrators and officers in grade "H" & above shall be authorised to send mass mail. Any mail sent to a group of above 20 addressees shall be considered mass mail. However, some key officers, in other grades depending on need, shall be authorised by functional directors to send mass mails.
6. Internet user/ owner of an e-mail account shall be responsible for protecting his account and PC from unauthorized use. He/ She will take all precautions in this regard. The owner of the e-mail account shall be held responsible, if his/ her account has been used to compromise the organisation, e.g. sending defamatory e-mail, use of harassment, unauthorised purchasing etc.



IndianOil

7. For all PCs on which Internet access facility has been given should have a defined 'owner', who could be held responsible for any violation of e-mail or Internet usage policy from that PC. This would also apply to all user accounts who will be responsible for e-mail and Internet usage from their respective accounts.
8. Use of email is strictly prohibited in the following respects:
 - a. Sending or forwarding unnecessary messages or other non-work items particularly to several people.
 - b. Sending or forwarding material that could be construed as confidential to such recipients who are not authorised to receive the same.
 - c. Sending or forwarding political, profane, obscene, threatening, offensive or libellous emails.
 - d. Sending or forwarding messages for purposes constituting clear conflict of company interests and policies or violation of company's security policy.
 - e. Broadcasting unsolicited personal views on social, political, religious or other non-business matters.
9. In case any employee is observed to be violating above guidelines, his/her e-mail/internet access will be barred without assigning any reason, besides appropriate action as deemed fit.
10. IOCL encourages the use of electronic mail and does not wish to inspect or monitor electronic mail routinely or to be the arbiter of its contents. Nonetheless, the electronic mail and data stored on the IOCL mail network of computers may be accessed by the Company or its authorized representative, for the following purposes:-
 - > Troubleshooting hardware and software problems
 - > Preventing unauthorized access and system misuse
 - > Retrieving business related information from an mail account
 - > Complying with legal requests for information
 - > Rerouting or disposing of undeliverable mail

The above policy guidelines come into force with immediate effect and may be brought to the notice of all concerned.

(VC Agrawal)
ED (HR)

Confidential

CC: ED (IS & OPTIMIZATION), CO / GM (IS), CO / GM (IS) PL HO/ DGM (Systems), Mktg
HO / DGM (IS & AD), R&D Centre, / CM (IS) Ref HQ :

- For retrieving business-related information from an email account, the e-mail Administrator will need the approval of the Head-IS to access specific mail and data for these purposes. The Head of IS group will keep HOD of the concerned employee informed about the same. The extent of the access will be limited to what is reasonably necessary to acquire the information.
- Complying with legal requests for information may be done with the approval of respective Head of the Unit/State/Region.
- Necessary action may be taken to mitigate e-mail spoofing & authentication attacks
- These policy guidelines may be included as a part of IS Security Policy. Copy of Corporate planning note, forwarded by Dir (BD) on security measures to be provided, is enclosed for necessary action.



IndianOil

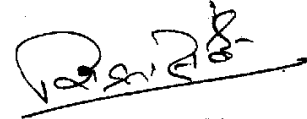
Ref. No. : S-296/Admn

Date : 10.06.09

CIRCULAR

It is notified to all concerned that in order to secure and maintain secrecy of the information pertaining to the Company Business Affairs and also in compliance of recommendations of the Intelligence Bureau, using personal Pendrive / Flashdrive in the office PCs and Laptops is not desirable. It has, therefore, been decided that henceforth, the Pendrive / Flashdrive used by an officer for official purpose should be authenticated by IS Department, in absence of which the USB Pendrive / Flashdrive would not work on any of the office PCs.

It is advised that all individuals using USB Pendrive / Flashdrive may please get their devices authenticated by IS Deptt. immediately.



(S.B.Singh)
DGM (A&W)

1. ED(M&I)/ED(F)/ED(PJ)/ED(PJ-PDRP)/ED(HR)/ED(PJ-PNCP&P15)/ED(SHIPPING/ED(Ops)-Offtg./GM(S&EP)/GM(PDEC)/DGM(HR)/DGM(HRD)/DGM(T&D)/DGM(IS)/DGM(MS)/CM(CC)-Ref. Hqrs., New Delhi
2. ED(IA)/ED(I/C)-IS/ED(I/C)-GAS/ED(CF)/ED(BD-R&P)/GM(I/C)-PC/ED(BD-F)/ED(CA)/ED(AAC)/ ED(HRD)/ED(HR)/ED(E&P)/ED(P&Tax)/CEO(IOF)/ED(IT)/GM(I/C)-CP&ES/GM(Co-ord)/ GM(RM)/GM(CC)/Convenor-Petrotech-2009 - CO, New Delhi
3. ED - IIPM, GURGAON
4. DGM/CEA/ES TO: CH /D(R)/D(F)/ D(PL)/D(M)/ D(HR)/ D(PLG&BD)/ D(R&D)/Advisor(Sec)/CVO
5. Notice Board