Information Technology Policy

Release Date – 25/02/2010

FOREWORD

Information Technology (IT) has immense power to impact global trade, culture and even governance. IT has permeated almost every aspect of our society today, changing the way we work, and will continue to do so in the future.

We realized the power of IT during its infancy in India, and hence have made regular investment to use IT to power our business growth. Information Technology in IndianOil has come a long way from being a data processing department to playing the role of business enabler today. Today, we have one of the largest data networks in India running one of biggest ERP set-up in South Asia. We have brought transparency to our employees, our customers and other stake holders by the efficient use of Information Technology.

Our focused initiative in making SAP successful has now expanded to make the whole IT ecosystem around SAP systems. This has enabled better and transparent flow of information to all our stakeholders. However, with such immense growth in usage of information, comes the responsibility of securing this information. Securing the vast information available in our organization is of pivotal interest in the growth of our organization in this competitive era. Information needs to be available to all our stakeholders at all the time in correct and desired manner. As a business leader, we also need to align our IT practices with the best in industry, to remain competitive and to bring out the best of cutting edge technology available to us.

With such focus, I am pleased to present the Information Technology policy to you. This IT policy provides the framework for the planning and deployment of cost effective, responsive and best practice Information Technology that-can support the achievement of Corporation's vision and minion statements. The IT policy places special focus on IT security, considering the threats our IT infrastructure faces-due to our important roles in moving the nation and managing its Petroleum security. I believe this IT policy will pmvide the necessary impetus towards implementing standard practices resulting in enhanced productivity and more transparency of information. At the same time, it would enable better protection of the information critical to our business needs.

I believe that this policy would be one of the comer-stones of o w business growth in future and help us in retaining our numero uno status.

On behalf of the Corporation, I acknowledge with thank the efforts and diligence of all individuals involved in formulating this Policy document.

(S. V. Narashiman)

Director (F)

Table of Contents

1. Vision

1.1. The Information Systems (IS) Group of Indian Oil Corporation Ltd. shall strive to bring reliable business information on a continual basis to the employees and Business Partners without compromising data integrity and security of the Corporation through the use of innovative and environment friendly technology, thus promoting corporation's Vision with Values.

2. Scope / Coverage

2.1. The purpose of this policy is to ensure an Information technology infrastructure that promotes the business needs of the Corporation. This policy intends to ensure,

- The integrity, reliability, availability and superior performance of Information Technology systems.
- That the use of IT Systems is consistent with business goals of the Corporation.
- That IT infrastructure is used for its intended purpose.
- And to establish processes for addressing policy violation and sanctions for violators.

2.2. This policy is applicable to users in all offices of IndianOil and its subsidiaries in India. Any item not forming part of this Policy shall be governed by Divisional IT Policy, if any. In case of any conflict with Divisional IT Policy, this policy shall supersede but shall operate within the framework of other Corporate Policies and Guidelines issued from time to time.

2.3. Requirements of Foreign offices shall be handled by individual divisions based on needs and local statutory mandatory requirements.

2.4. This policy along with IT Security Policy shall cover all activities related to IT. This policy supercedes all previous guidelines and circulars issued to this effect.

2.5. This Policy shall be reviewed and approved from time to time by the following three member committee.

a) ED (IS), COIS
b) ED (HR), CO
c) ED (CA), CO

2.6. This Policy shall be suitably amended in accordance with IT Act and other regulations passed by Government of India from time to time.

3. Procurement

3.1. While procuring IT related equipment, if the rate contract is available with DGS&D, Divisions can avail the same.

3.2. Procurement of any IT equipment by any other department which is going to be part of IOCL Network (LAN/WAN), shall have the involvement of IS department.

3.3. IS Department of Divisional HO shall decide the minimum configuration of Servers / Desktops and Notebook PCs on half yearly or on need basis and circulate the same for procurement.

4. Inventory Control

4.1. Each Division shall maintain detailed inventory of all IT related assets procured by IS Dept.

4.2. All IT assets like Hardware, Peripherals, Networking components, Software and Media etc. shall be suitably insured for Fire, theft, natural calamity etc.

5. Maintenance

5.1. All IT Hardware and Network components purchased shall have a 3 year comprehensive warranty. Any exception to this can only be made on specific approval from IS Head of the Division.

5.2. For Annual maintenance of all IT Hardware and Networking equipment procured/ maintained by IS department, the rates and Agency shall be finalised by COIS. However, Separate Agency shall be engaged by Divisions for specialised equipment procured/ maintained by IS Department.

5.3. Standard IT Hardware like PCs, Servers, Printers/Scanners, Switches, Routers etc. procured by other department subsequently added to IT Inventory shall be maintained by IS department.

5.4. Separate agencies may be engaged by individual Division for Facility management Services (FMS) comprising of – regular monitoring (console) of patch management, Antivirus updation , Internet traffic/bandwidth management, System administration of Firewall, Proxy, Content filter, AntiSpam device, all server/system administration etc.

6. Obsolescence

6.1. Desktops / Servers / Printers / Monitors / Routers /Switches and other IT related peripherals shall fall in the category of obsolete item which are either : -

- Phased out by the manufacturer (reached end of life EOL).

  OR
- They do not support technical advancement like higher / newer version of SAP, operating system (O.S.), system software, application software etc. that is likely to affect the business/ operational requirement of the corporation adversely.

  OR
- The equipment is beyond repairs (as certified by the AMC partner/OEM).

  OR
- Main components of the equipment e.g. CPU, RAM, HDD, Controller Cards, SMPS, main circuit boards etc. are no more available in the market.

  OR
- The equipment is beyond economical repairs e.g. cost of repair is more than 50% of the cost of similar new equipment

6.2. Notebook PC (laptop) to be considered obsolete as per clause 6.1. In addition, notebook PC may also be considered obsolete after 4 completed years from the date of purchase.

6.3. In case of replacement of obsolete item with new equipment, buy-back option shall be explored.

6.4. The required disposal procedure such as Administrative approval, write off approval etc. are to be followed as per procedure. However, decision to declare obsolete item is to be taken in consultation with respective unit IS Head.

7. Hiring

7.1. Necessary IT equipment can be hired for exceptional reasons like training, urgent replacement in lieu of breakdown of server, etc.

7.2. Hiring shall not be used to fulfill the permanent shortage of IT equipment.

8. Experimentation of Technology

8.1. To keep itself abreast with the changes in technology and take decision on adoption of the same. COIS/ Divisional IS can procure IT equipment on experimental basis for use.

8.2. After evaluation, Divisional IS shall give its report to COIS on usefulness of the technology.

9. Hardware

9.1. Allotment/Distribution.

- PC – One PC per seat for officers. If there are 3 officers coming in shifts for the same job, they shall share one PC but use their own login ID not common user login ID. Allocation of PC for staff shall be approved by the HOD/Functional Head.
- Notebook PC – Each Division shall draw its own policy for allotment of notebook PC.
- Printers – Use of shared LaserJet printers on LAN shall be encouraged. Individual printers can be given only to the officers on need basis in exceptional cases approved by the HOD/Functional Head.
- Scanners, CD/DVD Writers and other peripherals can be provided on need basis. The proposal for the same must be approved by HOD/Functional Head.

9.2. Change in the configuration by way of increasing memory and Hard Disk Capacity – On exceptional basis and where need exists, memory and storage capacity can be increased for individual PCs and notebooks. Such proposal needs approval of functional HODs in consultation with unit IS Head.

10. Software

10.1. All Desktops/Servers/Laptops shall have licensed and authorized software.

10.2. All SAP Software Licenses shall be procured centrally at COIS and shall be distributed as per requirement. Other standard software such as Anti Virus, OS, Application Software and Data Bases etc. shall be procured by divisions.

10.3. Office automation software – MS Office: Agency and rate contract for licenses shall be finalised by COIS for bulk requirement.

10.4. **Maintenance**.

- COIS shall arrange for renewal of subscription for all software procured by them. For other software respective Divisions shall arrange for renewal.

10.5. Disposal.

- Adequate measures shall be taken to prevent misuse of obsolete Media and licenses.
- Whenever a PC or a server or a Hard Disk is replaced or reallocated, all user generated documents, images and files shall be removed before reallocation, the responsibility for ensuring this shall be borne by the individual whose PC has been replaced, in coordination with the engineer who moves that person’s files to the new machine.
- A replaced Machine shall also have all installed software removed before re-distribution.

10.6. Inventory of all the software and licenses must be maintained by all the locations.

11. Communication (LAN & WAN)

11.1. Every Division shall arrange for procurement of necessary hardware for networking, except VSAT equipment, as per specifications finalized by COIS from time to time, unless decided otherwise by COIS.

11.2. No leased line, MPLS VPN line, ISDN line and point to point RF WAN link between locations can be provided without prior approval from COIS.

11.3. Rate contract and Agency of MPLS services for WAN shall be finalised by COIS.

11.4. Line bandwidth can be enhanced or reduced as per the requirement of the respective Divisions. However COIS shall be duly informed of such changes.

11.5. Adequate security measures like Firewall, IPS etc. must be in place to extend LAN beyond office building.

11.6. IP Address scheme and allocation for LAN /WAN shall be governed by COIS.

12. Consumables

12.1. Consumable like Cartridges, floppies, CDs, DVDs, pen drive etc. shall be treated as stationary items and shall be procured accordingly.

13. Web Site – Hosting and Domain name Management.

13.1. All websites shall be hosted in-house or NIC, ERNET or any other server owned by Government of India or the State Government or with a third party organization's servers located in India or as per prevalent guidelines on subject issued by Govt. of India.

13.2. Domain name registration and renewals shall be done by COIS/Divisional HQ.

14. SAP Access

14.1. SAP user accounts shall be created on need-to-use basis on the approval of Competent Authority not below the rank of GM.

14.2. The usage of the SAP Licenses shall be closely monitored by COIS.

14.3. The user accounts shall be disabled on non-usage for three months, and revalidation of thus disabled accounts shall go through standard new user creation process.

14.4. The other SAP Access Policy shall be governed by approved "Security and Authorization policy of SAP" maintained by COIS.

15. Internet Connectivity.

15.1. Divisions shall provide Internet connectivity with adequate security measures.

15.2. Desktop/notebook in any LAN shall not be permitted to be connected to the Internet through any attachment of any modem (broadband/ LL/ cable/ PSTN), or data card etc.

15.3. Internet usage and e-mail shall be governed by the Policy given in **Annexure – A (I).**

16. E-mail Accounts

16.1. Every officer shall be entitled for an email account. Email account for staff can be generated on need basis and shall be approved by an officer not below the level of GM.

16.2. All users shall be encouraged to archive their email on local storage.

16.3. Email more than two months old shall automatically be deleted from the server with a warning prior to deletion.

16.4. Each user shall get storage of minimum 50 MB to store his emails on server. Capacity of higher mail box size shall be decided by the Divisional IS Head.

16.5. All emails shall be scanned for virus and spam to remove junk mails.

16.6. Maximum number of recipients per mail shall be limited to 20.

17. Security

17.1. The e-security policy shall have details about all security aspects related to Information Systems and is enclosed as **Annexure - A**.

17.2. All Servers/PCs shall be adequately protected from threats like virus, spam, malware, malicious software etc. Necessary measures to be adopted to provide the same.

17.3. To detect malicious activities in the network, IDS/IPS and vulnerability management system shall be installed. OS patches shall be updated as per the guidelines of the OS manufacturer to avoid security threats, through deployment of appropriate tools.

17.4. External Notebooks:

- It must be ensured that any external Notebooks, if connected to IOCL LAN are free of virus in order to protect the IOCL network.

17.5. Usage of Pen drives :

- Pen drives shall not be allowed to be connected to the Notebooks/Desktops, which are connected to IOCL network, unless it is authenticated for use, as per HR policy enclosed as Annexure - B.

18. Active Directory Group Policy.

18.1. Security policies as defined in Annexure–A shall be implemented as a Group Policy through Active Directory (AD).

19. Training

19.1. Each Division shall draw its annual training calendar and share it with other divisions. This calendar shall consist user training and skill up-gradation training for employees from IS department. Any employee can be nominated across divisions for relevant training.

19.2. Employees from other departments can be nominated for IS related training. This shall be approved by respective Head of IS department.

19.3. IS Head can nominate any employee for outside seminar and training & Certification as per training policy of the respective Division. Such approvals shall be routed through respective training departments.

19.4. IS Head can nominate any employee for outside seminar and training which does not require any subscription. Such nomination shall not need approval from training department.

19.5. User Training shall be conducted on regular basis about awareness of e-security practices.

20. Trainees – Apprentice & Summer Trainees.

20.1. The Divisional IS at HQ and other units having IS Departments can engage Apprentice / Summer Trainees.

20.2. Apprentice.

- Students doing course from Technical / Educational institutes which requires on the job training as a part of its curriculum and whose training period is minimum eleven months can be engaged as apprentice trainees.

- These trainees shall be paid the same stipend as paid to apprentice doing Chartered Accountancy and are taken by Finance Department.

20.3. Summer Trainees.

- Students pursuing engineering degree in Information Technology related courses can be taken as summer trainees to fulfill their curriculum needs.
- Acceptance and selection of these students shall be done by respective Training departments. Each student shall be allotted one guide / mentor from IS Department. Each student shall be given a project as per his need. No stipend shall be paid to these summer trainees.
- Training Departments shall supervise the progress of the student with periodic review.
- At the completion of the project, Training Department shall issue necessary certificates for submission to the college.

20.4. Summer Trainees shall not be engaged in COIS.

21. Usage Policy

21.1. This usage policy applies to all users of all IT systems, including but not limited to employees and approved agencies. This policy also applies to privately owned computers when connected to the corporate network.

21.2. IT systems may be used only for their authorized purposes.

21.3. Users are entitled to access only those areas for which they have authorization.

21.4. The following categories of use are prohibited :

- To deny or interfere with or attempt to deny and interfere with services to other users in any way, including resource hogging, misusing mail list, propagating chain letters or virus hoaxes, spamming (spreading email widely and without good purpose) or bombing (flooding an individual, group or system with numerous or large email message) and distribution of unwanted mail.
- Attempts to compromise system security.
- Unauthorized access or use.
- Disguised use.
- Distributing computer viruses.
- Modification or removal of data or equipment.
- Use of unauthorized devices.
- Illegal use of IT systems.
- Use in violation of corporate contractual obligations including limitations defined in software and other licensing agreements.

21.5. Users shall be responsible for maintaining security of their own IT system accounts and passwords. User accounts and passwords shall not be shared.

21.6. Upon request from IS personnel, user shall produce valid identification.

21.7. Corporation reserves the right to access all aspects of IT systems without informing the user.

21.8. IS Department shall deactivate the user access, if the user is suspected of violating the IT Policy.

22. Disciplinary process for violation of Policy

22.1. Any violation of Policy on Information Technology shall be reported to Head of IS Department at the Divisional Head Office, who shall report the matter to HR Department for appropriate action.

23. Management of Computer Centre

23.1. Computer Centers shall maintain a temperature of less than 22 degree centigrade.
23.2. Apart from centralized AC, Window/split AC of appropriate tonnage shall be installed as backup.
23.3. Servers, networking equipment and any other important equipment at computer center shall get power from online UPS.
23.4. The capacity of the UPS for the computer center shall be decided by the respective IS Department.
23.5. Adequate safety measures shall be provided in consultation with S&EP Department.
23.6. Network audit, IT Security Audit (vulnerability test) and IT process audit shall be carried out once a year.
23.7. Physical / General Safety.

- Routers and switches etc. shall be housed in network racks.
- Location-in-charge shall be responsible for providing safety, security, proper upkeep and ambient environment for IT equipment placed at their location (e.g. A/C dust/ dirt free environment etc.)

24. Business Continuity Plan & Retention of Data.

24.1. Business Continuity plan.

- Divisions shall ensure that a backup system is installed. Detailed documentation for backup and recovery procedures shall be maintained. Register / log shall be maintained for backup taken.
- The system shall be able to take automated backup of open and closed files.
- The backups so taken shall be verified periodically.
- The media in which backup is taken shall be kept in a fireproof cabinet and kept at a different geographical location, so that the backup media is available elsewhere for restoration and use, in case of any calamity like fire, flood etc.
- For important data and data being changed regularly, at least two sets of backup for alternate day shall be available.
- IS department shall be responsible for safekeeping of corporation’s business data which are stored in the servers of IS Department.

- Individual PC users shall be responsible for keeping back up of their own data.
- Retention of Data :-

  Electronic data shall be retained for minimum of 7 years. However, wherever data is required for longer period due to any ongoing legal issues, the same may be retained as per the requirement of the concerned functional department.

	25/02/2010	25/2/10	25/02/10
A. R. Paranjpe (Marketing)	S.L. Agarwal (R & D)	S.K. Majilya (Refineries)	Sandeep Kr Singh (Pipelines)
25/02/10.	25/2/10		25/2/10
Bhupendra Kumar (COIS)	S.B. Deshpande (COIS)	G.R. Babu (COIS)	Rajiv Chawla (COIS)

Annexure - A

e-Security Policy,

&

Internet Usage Policy

1. Policy Statement.

"It shall be the responsibility of the IS Department to provide adequate protection and confidentiality of all corporation data in electronic form and proprietary software systems to ensure the continued availability of data and programs to all authorised users and to ensure the integrity of all data and configuration controls."

General Security Policies.

1.1. Confidentiality of all data is to be maintained through Policy based and mandatory access controls.

1.2. Internet and other external service access shall be restricted to authorised personnel only.

1.3. Access to data on all laptop computers shall be secured through boot password, to provide confidentiality of data in the event of loss or theft of equipment.

1.4. Only authorised and licensed software shall be installed, and installation shall be performed by IS Department representative only.

1.5. The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it shall be removed from the workstation immediately.

1.6. It shall be the responsibility of the user to check all removable and portable media for virus before they are used within the Organisation.

1.7. Access to workstation shall be user based. User accounts shall be managed through Active Directory (AD).

1.8. Workstation configurations shall be changed by authorized IS Department representative only.

1.9. To prevent the loss of availability of IS resources; measures must be taken to backup data and applications held centrally. It shall be the responsibility of the user to backup the data on his/her desktop and notebook.

1.10. Employees shall be accountable for any breaches of the Organisation's Security Policies.

2. Virus Protection

2.1. Corporate file-servers shall be protected with virus scanning software.

2.2. Workstations shall be protected by virus scanning software.

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 that is brought in from outside the Organisation is to be used until it has been scanned.

2.5. All demonstrations by vendors shall be run on their own machines.

2.6. New customized software shall be scanned before it is installed as it may contain viruses.

2.7. Users shall be kept informed of current procedures and policies through User Guidelines.

2.8. 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 and any removable media or other workstations to which the virus may have spread and eradicate it.

3. Electrical Security

3.1. All servers shall be supplied conditioned power supply through UPS.

3.2. All network equipment shall also be supplied power through UPS.

3.3. In the event of a mains power failure, the UPS shall have sufficient power to keep the network and servers running until the generator take over.

3.4. Electrical audit shall be carried out once a year.

4. Inventory Management

4.1. The IS Department shall keep a full inventory of all computer equipment and software in use throughout the Data Centre.

4.2. Computer hardware and software audits shall be carried out periodically. These audits shall be used to track unauthorised copies of software and unauthorised changes to hardware and software configurations.

5. Access Control

5.1. SAP Access Policy shall be governed by approved “Security and Authorization policy of SAP” maintained by BASIS Group. It shall be applicable for all SAP usage. For all other log-ins following policy shall be applicable.

5.2. Users shall only be given sufficient rights to all systems to enable them to perform their job function.

5.3. Where possible no one person shall have full rights to any system. The IS Department shall control network/server passwords and system passwords shall be assigned by the system administrator in the end-user department.

5.4. Access to the network/servers/workstations and systems shall be by individual username and password.

5.5. Usernames shall be employee number based and fully integrated with AD.

5.6. All users/Administrators shall have a password of at least 6 characters.

5.7. Passwords shall expire every 90 days and must be unique.

5.8. The last three passwords that were chosen by the user shall not be reused.

5.9. The user/Administrator account shall be locked after 3 incorrect attempts.

5.10. User/Administrator Account shall be locked after 15 minutes of idle period.

5.11. User’s rights to all systems shall be removed as soon as possible on separation from the Organisation.

5.12. Network/ Server supervisor passwords and system supervisor passwords shall be stored in a secure location in case of an emergency or disaster, *e.g.* a fire safe in the IS Department.

5.13. Auditing shall be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.

5.14. IS Department representative shall not login as root on to UNIX, Linux systems, but shall use the su command to obtain root privileges.

5.15. Use of the admin username on Novell systems and the Administrator username on Windows is to be kept minimum.

5.16. Default passwords on systems such as Database servers, *etc.* shall be changed after installation.

5.17. On UNIX and Linux systems, rights to rlogin, ftp, telnet, ssh shall be restricted to IS Department representative only.

5.18. Common users shall not be given access to the UNIX or Linux shell prompt.

5.19. File systems shall have the maximum security implemented that is possible.

6. Server Security

This section applies to Windows, UNIX and Linux servers.

6.1. Access to the system console and server disk/tape drives shall be restricted to authorised IS Department representative only.

6.2. The operating system shall be kept up to date and patched on a regular basis.

6.3. Servers shall be checked daily for viruses, event logs, application logs and free space.

6.4. Servers shall be placed in a secured room.

6.5. Remote management passwords shall be different to the Admin/Administrator/root password.

6.6. Users possessing Admin/Administrator/root rights shall be limited to trained members of the IS Department representative only.

6.7. Use of the Admin/Administrator/root accounts shall be kept to a minimum.

6.8. Administrator shall change their passwords periodically and password change log file must be maintained.

6.9. User access to data and applications shall be limited by the access control features.

6.10. The system auditing facilities shall be enabled.

6.11. The number of concurrent connections shall be limited to 1.

6.12. System clocks of all servers in Data Centre shall be synchronised at least once a week.

UNIX & Linux Specific Security

6.13. IS Department representative requiring root access must make use of the su command.

6.14. Use of the root account shall be kept to a minimum.

6.15. All UNIX and Linux system accounts shall be password protected.

6.16. rlogin facilities shall be restricted to authorised IS Department representative only.

6.17. ftp facilities shall be restricted to authorised IS Services representative only.

6.18. telnet facilities shall be restricted to authorised users.

7. Workstations Security

7.1. Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows workstations may be locked.

7.2. All unused workstations shall be switched off outside working hours.

8. LAN Security

Routers & Switches

8.1. LAN equipment shall be kept in secure rooms. Hub rooms shall be kept locked at all times. Access to these rooms shall be restricted to authorized IS Department representative only.

Wiring

8.2. All network wiring shall be fully documented.

8.3. All unused network points shall be de-activated when not in use.

8.4. All network cables shall be periodically scanned and readings recorded for future reference.

8.5. Users must not place or store any item on top of network cabling.

8.6. Redundant cabling schemes shall be used where possible.

Monitoring Software

8.7. The use of LAN analyser and packet sniffing software is restricted to the IS Department.

8.8. LAN analysers and packet sniffers shall be securely locked up when not in use.

8.9. Intrusion prevention systems shall be implemented to prevent unauthorised access to the network.

9. Wide Area Network Security

9.1. TCP/IP shall be used as protocol for WAN.

9.2. Following routing protocols shall be used for TCP/IP routing,

- OSPF
- RIP ver 2
- BGP
- Static Routes

9.3. Wireless LAN's shall make use of WPA2 enterprise for encryption and authentication.

9.4. Users shall not install their own wireless equipment under any circumstances.

9.5. Dial-in modems shall not be used. If a modem must be used dial-back modems shall be used. A secure VPN tunnel is the preferred option.

9.6. Where leased lines are used, the associated channel service units shall be locked up to prevent access to their monitoring ports.

9.7. All network equipment shall be kept locked up in secure areas.

9.8. Unnecessary protocols shall be removed from routers.

9.9. The preferred method of connection to outside Organisations is by a secure VPN connection, using IPSEC or SSL.

9.10. All connections made to the Organisation’s network by external organisations shall be logged.

9.11. Network equipment shall be configured to close inactive sessions.

10. TCP/IP & Internet Security

10.1. Permanent connections to the Internet shall be via the means of a firewall to regulate network traffic.

10.2. Permanent connections to other external networks shall be via the means of a firewall to regulate network traffic.

10.3. Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) shall be used.

10.4. Workstation access to the Internet shall be via the Organisation's proxy server and website content scanner.

10.5. All incoming e-mail shall be scanned by the Organisation's e-mail content scanner.

11. Remote Access Security Policy

Wireless Access

11.1. Where the network is accessed remotely via wireless appropriate wireless security standards shall be used.

- WPA2 enterprise shall be used as standard on Wi-Fi connections.
- A WPA2 encryption key shall be used.
- The network shall be configured not to advertise its presence.
- Due to the possibility of cracking Wireless Encryption Protocol using sniffing software such as AirSnort all wireless access points shall be outside the firewall.
- Users shall not install their own wireless devices in the office LAN / equipment under any circumstances.

11.2. Secure Access via VPN

Access from remote users to the corporate network shall be via secure IPSEC VPN or SSL VPN connections only. This is necessary to secure the connection from the remote device to the corporate network.

11.3. Two factor authentication shall be used for administrative users to access IOC network over Internet

11.4. Prevention of Data Loss

All laptops and PDA's that are taken off site shall have hardware password enabled to prevent data loss in the event of theft.

11.5. Remote Device Protection

To prevent remote PCs, laptops, PDA's *etc* from compromising the corporate network, security software shall be installed on the devices.

- Firewall software shall be installed on the devices to prevent them from being compromised by Trojans and back door software.
- Anti-virus software configured to automatically download the latest virus signatures shall be installed and utilised.
- Necessary measures like Network Access Control shall be used to protect Remote as well as local device from unauthorized access.

11.6. Access from Wireless devices shall be through Firewall only.

11.7. Blue Tooth

To prevent Bluetooth enabled devices from being attacked and compromised the Bluetooth connections on mobile phones, PDA's and laptops shall be disabled where appropriate. This is to prevent bluejacking, SNARF and backdoor attacks.

11.8. Standard Devices & Configurations

Devices that are used to access the network remotely, must meet the minimum standard for supported web browsers and operating systems that is current at the time of access.

11.9. Authentication

Authentication for remote access shall use two-stage authentication. As a minimum this shall comprise two-stage username and password verification.

Hardware/Software token authentication shall be used in conjunction with the user's password.

11.10. Hardened Corporate Applications

All corporate applications shall be hardened as much as possible, particular attention shall be paid to those applications, which are accessible remotely. The security features of applications shall be fully utilised and all security patches shall be applied.

12. Internet usage and e-Mail Policy

12.1. User access to Internet and e-mail shall be governed by the Policy given in **Annexure – A (I).**

13. User Responsibility

These guidelines are intended to help the users to make best use of the computer resources at their disposal.

a) Users are individually responsible for protecting the data and information in their hands. Security is everyone's responsibility.

b) Recognise which data is sensitive. If users do not know or are not sure, they shall ask System Administrator.

c) Every user must be aware that he/she is accountable for what he/she does on the system.

d) Mail facility shall be used for official purpose only.

e) Any PC may be audited periodically.

f) Logins to, and use of the Organisation's network are monitored and audited.

g) *Failure to comply with the organisation's security policy may lead to disciplinary action.*

14. Application Security

14.1 All customised application development shall follow basic secure coding practices.

14.2 All existing software applications not meeting the above criteria shall be modified in a phased manner to meet the requirements.

14.3 To avoid the misuse of the application the ownership of source code for all the application developed through outsourcing shall remain with the organization.

Annexure – A (I)

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. 29.10.2009 from ED (HR), CO attached below.

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.

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 8.0 below.

5.4 The Corporation can and shall 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 shall 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 our policies.

5.7 Such monitoring shall 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. Hacking into unauthorized areas.
g. Publishing defamatory and/or knowingly false material about the corporation, colleagues and/or our 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. Any other action that is prohibited by law.

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

7.0 Objectionable Material

7.1 Users shall not access/upload/download materials that can be deemed objectionable to other employees.

8.0 Misconduct

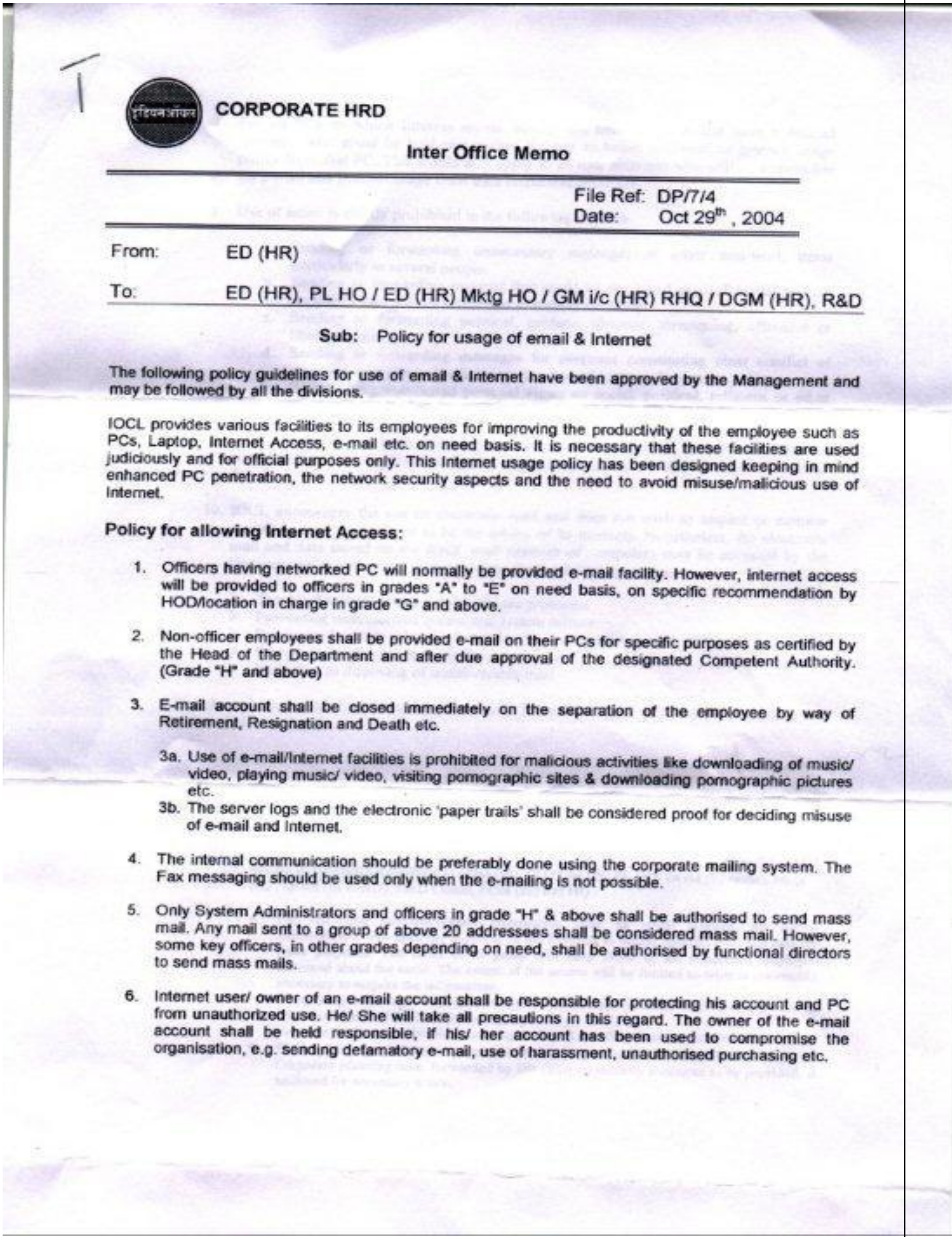
8.1 Where it is believed that an employee has failed to comply with this policy, he/she shall face the corporation's disciplinary procedure.

9.0 All the filtering appliance/software works based on global category of the site which is decided on certain parameters. Hence there are chances that valid business site is booked in wrong category. In CO-IS the sites have been blocked/monitored as per the list indicated below. However, based on usage pattern and threat perception the monitoring and blocking action for the category may be changed by the authorised IS-security personal.

Site Category	Monitor	Block
Abortion		
Pro-Choice		B
Pro-Life		B
Adult Material		
Adult Content		B
Lingerie and Swimsuit		B
Nudity		B
Sex		B
Sex Education		B
Advocacy Groups		
Bandwidth		
Internet Radio and TV		B
Internet Telephony	M	
Peer-to-Peer File Sharing		B
Personal Network Storage and Backup	M	
Streaming Media	M	
Business and Economy		
Financial Data and Services	M	
Drugs		
Abused Drugs		B
Marijuana		B
Prescribed Medications	M	
Supplements and Unregulated Compounds	M	
Education		
Cultural Institutions	M	
Educational Institutions	M	
Educational Materials		
Reference Materials	M	

Entertainment	M	
MP3 and Audio Download Services		B
Extended Protection		
Elevated Exposure	M	
Emerging Exploits	M	
Potentially Damaging Content	M	
Gambling		B
Games		B
Government		
Military	M	
Political Organizations		B
Health	M	
Illegal or Questionable		B
Information Technology		
Computer Security	M	
Hacking		B
Proxy Avoidance		B
Search Engines and Portals	M	
URL Translation Sites	M	
Web and Email Spam		B
Web Hosting	M	
Internet Communication		
General Email	M	
Organizational Email	M	
Text and Media Messaging	M	
Web Chat	M	
Job Search	M	
Militancy and Extremist		B
Miscellaneous		
Content Delivery Networks	M	
Dynamic Content	M	
File Download Servers	M	
Images (Media)	M	
Image Servers	M	
Network Errors	M	
Private IP Addresses	M	
Uncategorized	M	
News and Media	M	
Alternative Journals	M	
Productivity		

Advertisements		B
Freeware and Software Download	M	
Instant Messaging	M	
Message Boards and Forums	M	
Online Brokerage and Trading	M	
Pay-to-Surf		B
Racism and Hate		B
Religion		
Non-Traditional Religions and Occult and Folklore		B
Traditional Religions	M	
Security		
Bot Networks	M	
Keyloggers		B
Malicious Web Sites		B
Phishing and Other Frauds		B
Potentially Unwanted Software		B
Spyware		B
Shopping		
Internet Auctions	M	
Real Estate	M	
Social Organizations		
Professional and Worker Organizations	M	
Service and Philanthropic Organizations	M	
Social and Affiliation Organizations	M	
Society and Lifestyles		
Alcohol and Tobacco		B
Gay or Lesbian or Bisexual Interest		B
Hobbies	M	
Personals and Dating	M	
Restaurants and Dining	M	
Social Networking and Personal Sites	M	
Special Events		
Sports	M	
Sport Hunting and Gun Clubs	M	
Tasteless	M	
Travel	M	
Vehicles	M	
Violence		B
Weapons		B



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.

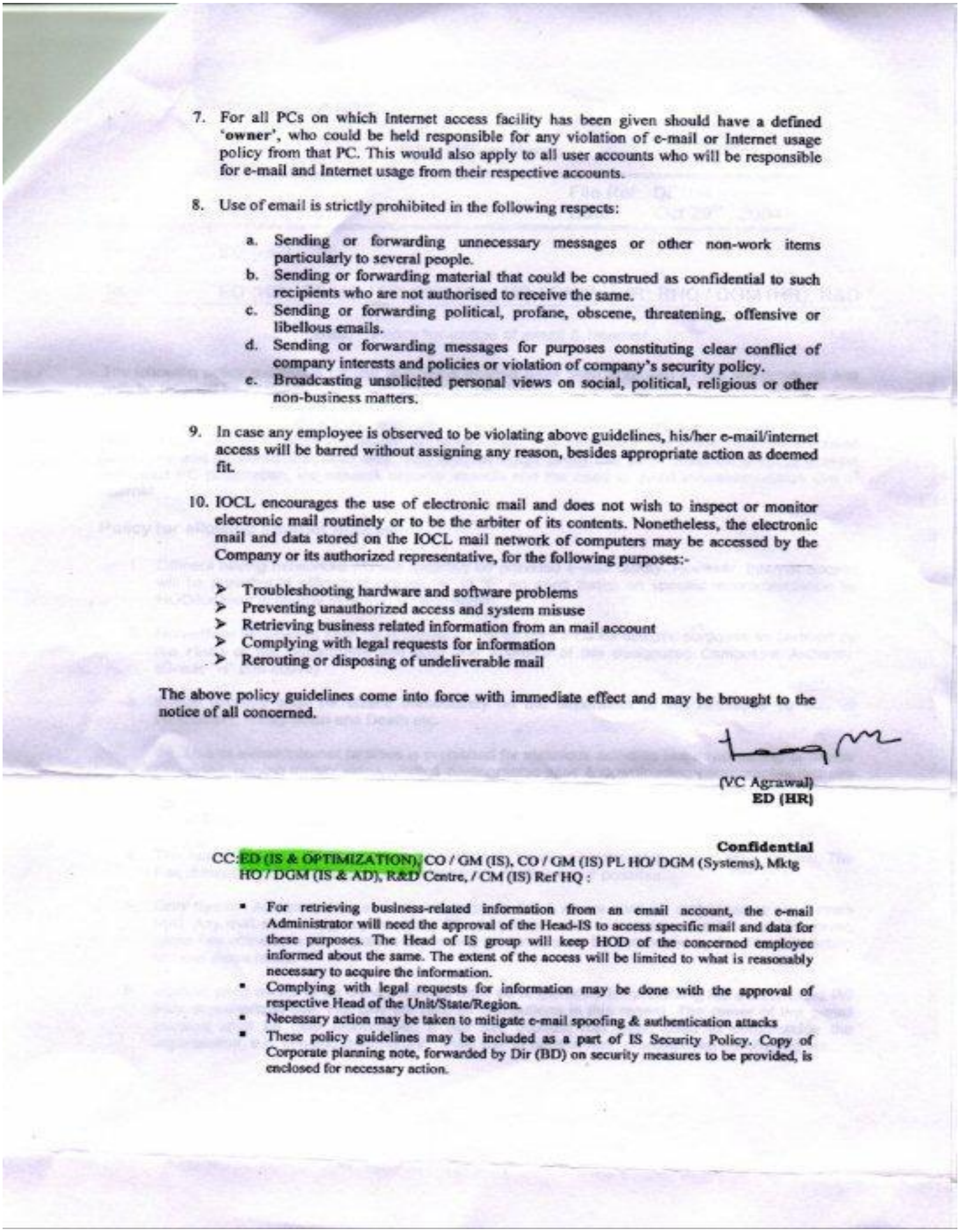
   3a. Use of e-mail/Internet facilities is prohibited for malicious activities like downloading of music/ video, playing music/ video, visiting pornographic sites & downloading pornographic pictures etc.

   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.



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)

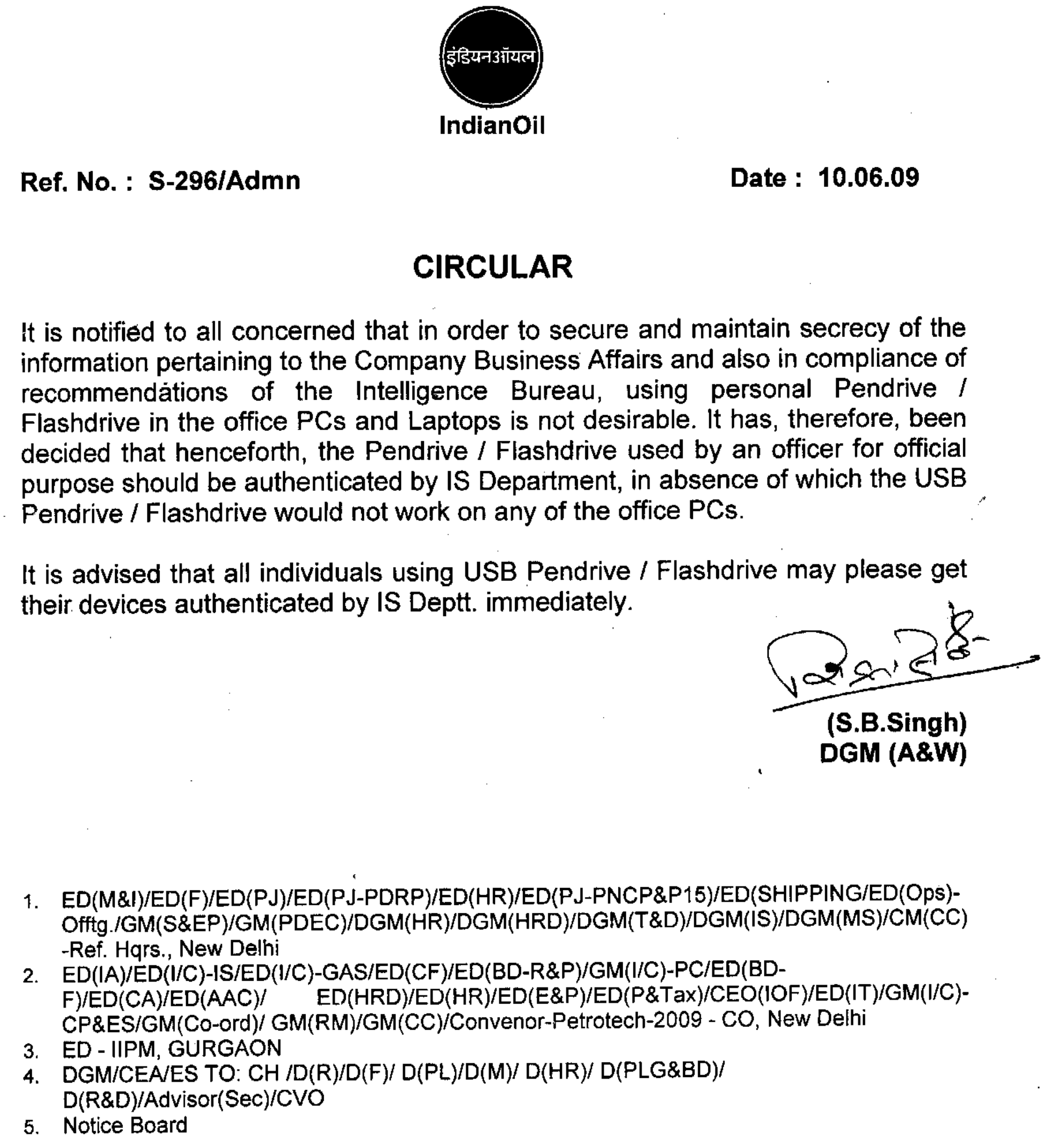
Confidential

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.

Annexure - B

Policy on Usage of Pen drives



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