INFORMATION TECHNOLOGY POLICY

(For USERS only)

INTERNAL

ITPO
(A Govt. of India Enterprise)
Pragati Bhawan, Pragati Maidan,
New Delhi – 100 001, India

Version -1.1

Notice of Distribution	This document is available to employees of ITPO. Any request to update this document must be authorised by SD&CS Division Division.
Notice of Confidentiality	This document contains proprietary and confidential information of ITPO. The recipient agrees to maintain this information in confidence and not reproduce or otherwise disclose this information to any person outside of the group directly responsible for the evaluation of its contents.

DOCUMENT SUMMARY:

AUTHOR	SYSTEM DEVELOPMENT & COMPLIANCE SERVICES DIVISION	
REVIEWED BY	GENERAL MANAGER – IT	
CURRENT VERSION	1.1	
DATE OF CURRENT VERSION		
DATE OF ORIGINAL VERSION		
DOCUMENT TYPE	POLICY	
DOCUMENT STATUS		
DOCUMENT CIRCULATION	NEED BASED CIRCULATION ONLY	
OWNER	ITPO	
APPROVED BY	NAME:	
	DESIGNATION	

REVISION HISTORY:

PARTICULARS	VERSION	REVISION NO.	DATE	EDITED BY/ REMARKS
CREATED	1.0		26.5.2014	
MODIFICATIONS	1.1	1	20.6.2014	

Table of Contents

1.0 PHYSICAL & ENVIRONMENTAL SECURITY POLICY

1.1 Objective

To prevent unauthorized access, damage and interference to business premises & information;
To prevent loss, damage or compromise of assets and interruption to business activities;
To prevent compromise or theft of information and information processing facilities

1.2 Preparing Premises to Site Computers

While selecting the premises, Administration department must ensure that computer equipment and data store is suitably protected from physical intrusion, theft, fire, flood and other environmental hazards. Capacity planning shall be done according to the number of systems to be housed and number of employees planned to occupy the premises, and a proper expansion plan should be made for future. The environmental requirements for the selected premises will be guided by the manufacturer's specification for housing the equipment. The following issues for implementing the above procedure:

- Malicious damage is likely to threaten the ability of organization to meet the business requirements and will result in unnecessary expenditure.
- The non-availability of the essential services such as power, A/C, water etc is likely to threaten the normal operations.
- Accidental damage to premises may threaten normal business operations.
- The theft of equipment would not only cause unnecessary expenditure, but may also disrupt the operation of critical systems.

1.3 Safety Equipment

Appropriate safety equipment is to be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment is to be checked regularly in accordance with manufacturers' instructions. Employees are to be properly trained in the use of safety equipment. Combustible computer

supplies such as stationery, other than immediate operational needs, should not to be stored within critical operations rooms.

1.4 Ensuring Suitable Environmental Conditions

Suitable environment control procedures shall be in place for smooth and reliable working of Information processing facilities. The environmental dangers that threaten the computer premises and the means by which they may be lessened or eliminated shall be aptly identified and implemented. Countermeasures or contingency procedures are to be defined for environmental hazards such as fire, smoke, water, dust, vibration, electrical supply interference.
Issues to be considered by the Admin for implementing the above procedure:

- Serious fire damage could make it impossible to continue business operations.
- Flooding can cause severe disruption to business in any form.
- Failure of air conditioning equipment can unsettle business operations and potentially result in halting of business output.
- Smoking, eating, and drinking is prohibited in computer equipment areas.
- Suitable Insurance Policy coverage for IT equipments.

1.5 Power Supplies

Equipment shall be protected from power failures and other electrical disturbances. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. Various options shall be considered to achieve continuity of power supply:

- Multiple feeds to avoid a single point of failure.
- Un-interruptible power supplies with n+n configuration
- Back-up generator

UPS equipment shall be regularly checked to ensure its adequate capacity and shall be tested with the manufacturer's recommendations. UPS shall support orderly close down or continuous running is recommended for equipment supporting critical business operations. There shall be SLA that ensures the maximum uptime with the supplier/contractor for maintaining of UPS.

1.6 Cabling security

Administration Division shall develop and implement the procedure for protection of power and telecommunication cabling. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception and damage. The following is an example of the security standards relating to cabling:

Issues to be considered for implementing the above procedure:

- Power and telecommunications lines to the information processing facilities shall be underground, where possible, or subject to adequate alternate protection.
- Network cabling shall be protected from unauthorized interception or damage.
- Power cables shall be segregated from communication cables to prevent interference.
- For sensitive or critical systems further controls to consider:
    - Installation of armored conduit and locked rooms or boxes at inspection and termination points.
    - Use of alternate routings or transmission media
    - Use of fibre optic cabling

Network cabling is to be protected from unauthorized interception and communications loss or damage by:

- use of conduits;
- Avoiding routes through public areas;
- Installation of locked rooms or boxes at inspection and termination points
- Implementation of secondary transmission media and/or routings.

1.7 Equipment maintenance & Security

System Administrator is responsible for developing the procedure for equipment maintenance. IT Equipments shall be correctly maintained to ensure its continued availability and integrity.

Issues to be considered for implementing the above procedure:

- Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications
- Manufacturers' instructions regarding the protection of equipment, such as its protection against exposure to strong electromagnetic fields, is to be observed at all times.
- Only authorized maintenance personnel shall carry out repairs and service equipment.
- Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate controls shall be taken when sending equipment off premises for maintenance. All requirements imposed by insurance policies shall be complied with.

IT equipment should be sited or protected to reduce the risks from environmental hazards and to minimize the opportunity for unauthorized access.

Critical equipment should be protected from power failures or other electrical anomalies.

1.8 Environmental Conditioning

Appropriate air conditioners are to be installed to maintain temperature and humidity for the computer centre.

- Temperature for the computer centre be continuously monitored and temperature should be maintained within the set limits
- Humidity in the computer centre should be maintained within set parameters
- Regular checks are to be recorded and routine preventive maintenance schedule has to be executed
- Supply air should be dust free and filtered before reaching the computer centre

2.0 SOFTWARE & HARDWARE POLICY

2.1 Objective

a) Enhance the uniform performance of the System Division in delivering, implementing, and maintaining software and hardware suitable to the business needs
b) Define the duties and responsibilities of organization employees who use the aforementioned software and hardware in the performance of their job duties.

2.2 Purpose

This policy addresses ITPO's intent to safeguard computing resources from various internal threats. This policy shall underline appropriate user etiquette for software and hardware usage and define procedures for safeguards.

2.3 Acceptable use

Hardware devices, software programs, and network systems purchased and provided by the organization are to be used only for processing organization-related materials, and other tasks necessary for discharging one's employment duties. Violations may result in disciplinary action in accordance with organization policy. Failure to observe these guidelines may result in disciplinary action by the organization depending upon the type and severity of the violation, whether it causes any liability or loss to the organization, and/or the presence of any repeated violation(s).

2.4 Hardware & Software Ownership

All Hardware & software acquired for or on behalf of the organization or developed by organization employees or contract personnel on behalf of the organization is and at all times shall remain organization property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

2.5 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on organization computers.

2.6 Outside equipment

No outside equipment may be plugged into the organization's network without the system division's written permission.

2.7 Offsite Security of Personal Computers/Laptops

Equipment used outside of organization premises must have the same protection as office equipment.

In particular:

- Password and virus controls must be in place.
- Equipment or media must not be left unattended in public or while traveling.
- Equipments should be protected against exposure to strong electromagnetic fields, or other hazards listed by manufacturers.
- PC is protected through "Power ON" password.

2.8 Inventory Management

The Inventory Management will help organization in identifying and controlling all its systems and will also enable it to take effective measures against identified unauthorized systems, if any.

- Manage inventory of all authorized organization systems (Hardware, Software and Networks) on ongoing basis across all ITPO offices / branches.
- Make a single person responsible for maintaining the Inventory at all ITPO offices/branches.
- Periodically update inventory.
- As far as possible, standardize the hardware and software used by ITPO.

- Care will be taken to ensure that the equipments and media will be cleared of all data residing thereon, before being disposed on account of obsolescence, damage etc.
- Each system (Hardware, Software and Networks) will have an owner who will be responsible for protecting and maintaining the owned system. He/She would also be responsible for reporting on any malfunctioning, damage, loss etc. in connection with the said system for remedial actions.

2.9 Distribution policy

The officers of the rank Deputy Manager and above shall be given a computer to perform the office work. The other officials shall be provided a computer based on the requirement and recommendation of the concerned HOD and GM IT.

2.10 Replacement policy

Computers/printers shall be replaced after a span of Six (6) years.

2.11 Retention policy – In order to reduce the carbon footprint and maintenance cost and to develop an eco friendly policy it is provisioned that after the usable span of Six (6) years the computers/printers may be sent to Stores Division for onward disposal. No retention shall be allowed by any officer/official.

In case of physical items in possession with the employees issued for personal use, such as mobile phone, laptop etc. but not returned to ITPO at the time of superannuation or retirement, the depreciated monetary value as applicable, will only be recovered.

3.0 PASSWORD POLICY

3.1 Objective

To prevent unauthorized user access;
To ensure protection of networked services;
To prevent unauthorized computer access.

3.2 Purpose

Passwords are one of the principal means of validating a user's authority to access a computer service. Password management

systems should provide an effective, interactive facility, which ensures quality passwords are maintained. A poorly chosen password may result in the compromise of entire corporate network. As such, all employees with access to systems are responsible for taking the appropriate steps, to select and secure their passwords.

3.3 Policies in detail

When deciding to make both the password and account lockout policies for computers and/or in the domain, consideration should be given for both the needs and abilities of the users. If the settings make passwords too difficult, and users are not adept at creating and remembering passwords, the policies may in fact be compromised by frustrated users who write passwords down and leave them under the keyboard or in a desk drawer.

3.4 User Accountability

Users are responsible for ensuring their passwords are:

- Passwords must be :
  - Kept confidential and individually owned. They should NOT be shared with other users
  - Not written down, except for lodging with departmental security staff or secure safekeeping, where appropriate
  - Changed whenever there is any indication of possible system or password compromise
  - Not talked about in front of others
- Not based on:
  - Dates, such as birth dates, anniversaries, etc;
  - Company names, identifiers or references;
  - User ID, user name, group ID or other system identifier;
  - More than two consecutive identical characters; or
  - All-numeric or all-alphabetic groups.
  - Telephone numbers or similar all-numeric groups; and
  - Not stored in any automated logon process, macro, or keyboard function key;
  - Not reused between different systems.
- Passwords must not be:
  - Shared with other users;
  - Revealed to family members, co-workers and boss;
  - Repeating sequences of letters or numbers;

- Names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names);
- The same as the user id;
- Stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

3.5 Temporary passwords

Systems are to be configured to ensure that the initial, temporary passwords for newly allocated accounts are changed at the first logon, and a record of the last five passwords for the account should be maintained to prevent password reuse. Default vendor passwords are to be removed immediately following installation of software.

3.6 Password display and storage

Passwords are not to be displayed on the screen when being entered, and the password verification file is to be stored separately from the main application system data. Passwords in this file should be stored in encrypted form, if possible, using a one-way encryption algorithm.

3.7 Password

This setting regulates how many different passwords must be used before the user can reuse one of them. The history should have 15-20 passwords. (The exact amount will be dependent on the max. age setting, below).

3.8 Maximum password age

This setting controls how long a password is good before a user is forced to pick a new one. The setting should be between 15 days to 30 days.

3.9 Minimum password age

This setting controls how long a new password must be used before it can be changed. This setting works hand-in-hand with the

password history setting above. This setting should be between 5 days to 15 days.

3.10 Minimum password length

This setting controls how many characters must make up the password. A strong setting would be 8 characters for normal user and 16 for administrator.

3.11 Account lockout duration

Once an account becomes locked out, through too many incorrectly entered passwords, this setting specifies how long before the account automatically becomes available again. A strong setting would be 30 minutes.

3.12 Account lockout threshold

This setting specifies the number of tries that a user (or intruder) gets to enter in an incorrect password before the account becomes locked out for the above-specified time. A strong setting should be 3 attempts.

3.13 Reset account lockout counter after

Each time an incorrect password is entered for an account, the setting above increments a counter. If this counter isn't set to decrement using this setting, the user account will be locked out after the threshold above has been reached, even if it takes years to reach the threshold. A strong setting is 120 minutes.

It is a recommended to document the existing settings before changing any of the policy settings, password and account lockout.

3.14 User-ids and Passwords

A password must contain characters from at least all of the following four categories:

Upper case letters, Lower case letters, Numbers, Special characters (e.g.: $, #, or punctuation characters such as? or!). Also, complex

passwords may not be made up of the username, or any part of the users' full name.

3.15 Multi-user systems

Each user of a multiple-user automated system shall be assigned a unique personal identifier or user-id. User identification shall be authenticated before the system may grant that user access to automated information. There should not be any anonymous accounts in any of the systems.

It may be noted that the aforementioned password mechanism is to be implemented in case no password implementation policy is advocated by the application service provider.

4.0 ANTI-VIRUS POLICY

4.1 Objective

To establish an antivirus security policy for the protection of all Organization information technology;
To protect the integrity of software and information.

4.2 Purpose

Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software and managers should, where appropriate, introduce special controls to detect or prevent its introduction.

4.3 General

- Anti-virus software scanning engine and the virus pattern files shall be kept up-to-date. The time of updating the virus patterns shall be kept minimized. The time frame acceptable for updating the new pattern file is 24 hours after the release of the patch.

- All computers of ITPO including servers, desktops & laptops shall have standard and supported anti-virus software installed.

- The virus scanner shall be scheduled to run to scan for viruses at regular intervals.

- Headquarters shall ensure that antivirus software is updated when a new antivirus definition/software release is available and when hardware/software compatibility is confirmed.

- Headquarters that maintains direct Internet access shall implement an antivirus system to scan Internet web pages, Internet e-mails, and File Transfer Protocol (FTP) downloads.

- Headquarters must comply with the requirements of the notification of credible computer threat events.

- Only authorized personnel shall make changes to the antivirus software configurations as required.

- Virus-infected computers shall be removed from the network as soon as they are identified, until they are verified as virus-free.

- Central monitoring and logging console shall be deployed, to monitor the status of pattern updates on all the computers and to log the activities performed on them.

- All virus detection incidents shall be logged, along with the action taken. Quarantine, Deletion or Successful cleaning.

- All computers shall be configured to generate the alert at the central Anti-Virus(AV) monitoring station; the responsible AV teams stations and the infected computers screen.

- Information Security Manager/ System official at RO shall identify a person or a team that is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

- Formal procedures for responding to a virus incident shall be developed, tested and implemented.

- Virus incident response shall be regularly reviewed and tested.

- Hoax threats can deflect attention from the genuine viruses and other malicious code, increasing susceptibility to infection. The policy shall communicate the users not to mass mail any virus related hoax, but to forward the same to the relevant person identified by Information Security Manager/ System official at RO.

- Regular audit should be done in all the users' desktops / laptops on a periodic basis to ensure that proper and latest version of virus engines and the definitions files are running and no virus threat exists.

- User awareness shall be created for all employees of ITPO for virus clean systems

4.4 Antivirus Guidelines for Employees

Guidelines for employees to ensure a clean virus free system and to prevent spreading of virus/worms are:

- Automatic scanning process should be initiated during boot time

- Both inbound and outbound SMTP messages should be scanned for viruses

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

- Delete Spam, chain, and other junk email without forwarding.

- Never download files from unknown or suspicious sources.

- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

- Always scan a floppy diskette/Pen/USB drive from an unknown source for viruses before using it.

- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

- Any activities with the intention to create and/or distribute malicious programs into and from ITPO's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

- New viruses are discovered almost every day. Periodically check the *Anti-Virus Policy* and this Recommended Processes list for updates.

4.5 RESPONSES TO A VIRUS INFECTION

Helpdesk or Incidence Response Team at CO and System Official at RO must be contacted immediately when a computer has been infected with a virus.

The Resident engineer / System Official or the Anti-Virus service provider will be able to remove the virus. This may involve a visit to the work site or resolution may take place remotely if the technician can access the computer using screen-sharing software. If an Engineer is unable to remove a virus infection, the computer's hard drive must be reformatted and all software reinstalled using clean, licensed copies.

If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer will be immediately disconnected from the network until it is

serviced by a Technicians or Engineers who will then verify that the computer is virus-free.

5.0 EMAIL USAGE POLICY

5.1 Objective

Appropriate use of the E-mail services to transmit & ensure appropriate protection of the organization information and equipments by Internet connections;
To protect the organization against damaging legal consequences;
To educate the individuals who may use the E-mail with their responsibilities associated with such use; and
To ensure effective utilization of E-mail services.

5.2 Purpose

Electronic mail is being used for business communications, replacing traditional forms of communication such as telex and letters. Electronic mail differs from traditional forms of business communications by, for example, its speed, message structure, degree of informality and vulnerability to unauthorized actions. Consideration should be given to the need for controls to reduce security risks created by electronic mail.

5.3 Policies in detail

Every ITPO employee who uses computers and has a business use in the course of their regular job duties will be granted an Internet electronic mail address and related privileges.

The e-mail security policy should enforce the following:-

- The Company provides the e-mail system to assist employees in the performance of their jobs and its use should be limited for official Company business.
- Personal use of the e-mail system should never impact the normal traffic flow of business related e-mail. The Company reserves the right to purge identifiable personal e-mail to preserve the integrity of the e-mail systems.
- No employee, consultant or contractor should use the Company's e-mail system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or

company, or which may be harmful to Company morale. This includes forwarding any received e-mail.

- Examples of prohibited material include:

  Sexually explicit messages, images, cartoons, or jokes;

  Unwelcome propositions, requests for dates, or love letters;

  Profanity, obscenity, slander, or libel;

  Ethnic, religious, or racial slurs;

  Political beliefs or commentary;

or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

- No messages should be sent or received which concern illegal activities.
- The system may not be used for personal financial gain.
- Internal Company e-mail and other internal materials should not be forwarded to destinations outside the Company.
- The forwarding of chain letters is strictly forbidden. This includes those purporting to be for Charity or other good causes as well as those promising wealth or other personal gain. Also virus warnings come under the same exclusion; the majority of these are false. If you wish to check the truth of these messages talk to Systems department but do not under any circumstances forward these messages to anyone inside or outside the Company.
- The user logged in at a computer will be considered to be the author of any messages sent from that computer. Remember to log-out from or lock your computer if you will be away from your desk. Under no circumstances should you send e-mail from a PC that you have not logged into.
- E-Mail addresses should not be disclosed unnecessarily. If you give your address when filling in surveys or other questionnaires you will be at risk of receiving unwanted junk messages.

- You should not subscribe to e-mail lists, which are not company approved. The volumes of messages that can be generated are high and you have no control over the content, which may bring you into conflict with the conditions stated above.
- E-Mail should, normally, not be used to send large attached files, unless very urgent. Many e-mail systems will not accept large files, which are returned and may result in overloading the Company's own e-mail system. CD's should be preferred to send large amounts of data, whenever possible.
- Do not open attachments to e-mail messages unless you are expecting them, and even then exercise extreme caution.

5.4 Suggestive Recommendations

- ITPO business communications sent by electronic mail must be sent and received using this company electronic mail address.
- Unsolicited electronic mail transmissions to prospects and customers are prohibited.
- A personal Internet service provider electronic mail account or any other electronic mail address must not be used for ITPO business.
- When transmitting messages to groups of people outside ITPO, employee must always use either the blind carbon copy (bcc) facility or the distribution list facility.
- Emotional outbursts sent through electronic mail and overloading the electronic mail account of someone through a deluge of messages are forbidden.
- Electronic mail is a public communication method much like a postcard. All ITPO employees are suggested to refrain from sending credit card numbers, passwords, or other sensitive information that might be intercepted.
- ITPO staff must additionally employ a standard electronic mail signature that includes their full name, job title, business address, and business telephone number and disclaimer notice.
- In all messages, it should be remembered that e-mail is not a secure form of communication as it travels in clear text unless it is digitally signed and encrypted. The messages that you send will be passed over networks owned by other people. If the content of the message could cause problems for the

Company or cause financial loss should the contents become known, a more secure method should be used.

- No messages of any kind should be sent to multiple external destinations. This may be considered as 'spamming' which is an illegal activity in many countries. If the business requirement is to send an email to multiple recipients then it should be sent to a group address or as bcc.
- Uses external e-mail facilities like Gmail, yahoo etc. should not be used for official communication.

6.0 INTERNET USAGE SECURITY POLICY

6.1 Objective

Appropriate use of the Internet to transmit & ensure appropriate protection of the organization information and equipments by Internet connections;
To protect the organization against damaging legal consequences;
To educate the individuals who may use the internet with their responsibilities associated with such use; and
To ensure effective utilization of Internet.

6.2 Purpose

The wide array of new resources, services, and inter-connectivity available through the Internet all introduce new business opportunities, and new security and privacy risks. In response to the risks, this policy describes the ITPO official policy regarding Internet security and acceptable usage.

6.3 Policies in detail

Officials are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of competent authority. Internet access is monitored to ensure that officials are not visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security policies. All information received from the Internet should be considered to be suspect until confirmed by reliable sources. Officials must not place ITPO material on any publicly-accessible computer system such as the Internet unless the posting has been approved by competent authority. Users are prohibited from

establishing any electronic commerce arrangements over the Internet unless Information System and the Information Security department has evaluated and approved of such arrangements. Sensitive information, including passwords and credit card numbers, must not be sent across the Internet unless this information is in encrypted form.

The following controls should be considered:-

- ITPO will provide access to the Internet to all authorised employees to assist them in the performance of their jobs. The authorised users would be from CMD, ED, Directors, Secretariate, SGMs, GMs and their PAs, DGMs, Sr. Managers, Managers and Dy. Managers and Division workstation. For officials below the level of DMs the internet will be provided on the recommendation by concerned HOD and GM IT . Where access is provided, use should be limited to official ITPO business.
- No messages should be posted on any Internet message board or other similar Web based service that would bring ITPO into disrepute, or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as those for e-mail.
- You should not engage in any illegal activities using the Internet.
- The system may not be used for personal financial gain, nor should you host a Web site on any ITPO equipment without express permission.
- Your use of the system should not have noticeable effect on the availability of the system for other users. Therefore you should not participate in on-line games or have active any web channels that broadcast frequent updates to your PC, such as News Ticker service.
- You should not visit Web sites that display material of a pornographic nature, or which contain material that may be considered offensive. Websites related to social networking, gambling, hacker/hacking activities are also to be avoided. It is recognised that you may accidentally view such material from time to time, if this happens please contact IT department immediately.
- You should not download any files from the Internet, or capture any images that are displayed. If you require a file

from the Internet please contact Systems division – there may be any number of issues concerning copyright, viruses and overall functioning of the computer.
- You should not enter your e-mail address on a web site unnecessarily. If you give your address when filling in surveys or other questionnaires you will be at risk of receiving unwanted junk messages.
- The person logged in at a computer will be considered to be the person browsing the Internet. You must log-out from or lock your computer if you will be away from your desk. Under no circumstances should you browse the Internet from a PC that you have not logged into.

The company monitors and logs all Internet accesses by individuals and reserves the right to access and report on this information.

6.4 Connectivity

- Only dedicated proxy server/s will be used to control and protect ITPO network
- No client will be permitted to communicate with the Internet, except through ITPO proxy / e-mail server.
- Firewall server that may combine any of the services of a proxy server, packet filter and many other security-based services will be placed between organization network and Internet.
- Run no other services or software on WEB, Mail, FTP or firewall servers.
- Pass only restricted traffic such as HTTP, SMTP and POP3 from / to Internet.
- No client machine connected to the Internet will enable file sharing
- Close all ports other than which provide the pre-defined services.
- Close ports such as Net BIOS for receiving any traffic from the outside world, since such connections are used for internal communications.
- Identity and specifications of firewall product used in and out of network will not be disclosed.
- Use alerting software to detect intrusion attempts
- Users are advised to adhere to the policy while using external component for internet browsing.

7.0 INTRANET SECURITY POLICY

7.1 Objective

To protect the organization against damaging legal consequences;
To educate the individuals who may use the intranet with their responsibilities associated with such use; and
To ensure effective utilization of Intranet.

7.2 Purpose

The wide array of new resources, services, and inter-connectivity available through the Intranet introduce new business opportunities, and new security and privacy risks. In response to the risks, this policy describes the ITPO official policy regarding Intranet security.

7.3 Policies in detail

The employees are provided with Intranet access to perform their job duties, and to keep them informed about organisation policies, procedures and include office automation. Employees are advised to use Intranet effectively and as per the detailed policies listed below. Intranet access is monitored to ensure that officials are utilising it to do their jobs, and also to ensure that they continue to be in compliance with security policies. Employees must not place highly confidential ITPO material under any section of Intranet unless the posting has been approved by the competent authority. The establishment of Intranet pages is separately handled by an approval process.

The following controls should be considered:-

Business Use Only—The ITPO Intranet is intended to facilitate more efficient and more effective ways for ITPO staff to communicate and conduct business. Like other ITPO information systems, because it is intended for business purposes, personal use is permitted only if the approval of competent authority has been obtained.

Respecting Intellectual Property Rights—Although the intranet is an informal internal communications environment, the laws for copyrights, patents, and trademarks apply. Employees may post material to the intranet only after using the following steps:

- If material to be posted originates outside ITPO, written permission from the source must be obtained, and the source must be given adequate credit.
- If copyright infringement, confidential information disclosure, libel, defamation of character, or other possible legal issues could be involved, ITPO's legal counsel must approve the posting.
- Employees must independently confirm the material's accuracy, timeliness, and relevance to ITPO business.

Prohibited Content—ITPO secret information must not reside on either Internet or intranet servers.

Content Control—ITPO computer and communications systems are not intended for, and must not be used for the exercise of the participants' right to free speech. These systems, including the intranet, must not be used as an open forum to discuss ITPO organizational changes, business policy matters, or similar topics. ITPO management has the right to censor, delete, or amend any information posted to company's computers and networks, including the intranet.

Approvals for Postings— Before any information is posted to the ITPO intranet, the competent authority as designated, must approve. A formal change control procedure must be used for all changes to the content posted to the ITPO intranet, and this procedure must include documentation reflecting management approvals and archival storage of all prior versions of posted material.

Classification for Postings—The content posted to the ITPO intranet must be classified as either Public or Internal Use Only. Confidential or Secret information must never be posted to the intranet. Staff in the Information Security department must review all postings to the ITPO intranet quarterly to confirm that none of these postings contain Confidential or Secret information.

Legal Ownership Of Material Posted—Unless approved in advance by the competent authority, and explicitly noted on the intranet page, all content posted to the ITPO intranet is the property of ITPO.

Designated Information Owner—All content posted to the ITPO intranet must have a designated Owner. Contact information for this Owner must be clearly indicated on the page where the content appears.

Production Systems—All intranet servers are considered production systems and must comply with all the production system requirements. These requirements include the formal assignment of responsibilities, adequate training for staff working on the production system, at least two trained staff members who are trained and technically competent to manage the system, regular backups, and periodic upgrades of software.

Restricted Dissemination—The ITPO intranet is for the exclusive use of authorized persons and all information contained therein may be disseminated only to authorized persons. Employees must not forward information appearing on the intranet to third parties without going through the appropriate internal channels.

Relevant Standards And Resources—All ITPO intranet pages must conform to layout standards, navigation standards, legal wording standards, and similar requirements specified by the intranet approving authority. All personnel developing intranet sites must consistently observe the intranet style guide and use the resources found in the intranet implementation repository.

Connections to Production Systems—The intranet must not be used to provide real-time connections to any ITPO production information system that has extended user authentication access controls, which is anything beyond a fixed password and a user ID, unless the approval of the Information Security department manager has been obtained.

Connecting Systems to the Intranet—Before any computer system, network segment, or network access mechanism, such

as a modem, may be connected to the ITPO intranet, it must be deemed to have met the necessary security criteria established by the Information Security manager. These criteria include, but are not limited to,

- No connection to the Internet that is not guarded by an acceptable firewall,
- An acceptable user authentication system,
- An acceptable user privilege control system,
- An established change control process,
- A clearly-written definition of system management responsibilities, and
- Adequate operational documentation.

Server Approval—Before they are connected to the internal network, the network services manager in the Systems Division must preauthorize all ITPO intranet servers. This authorization process includes assuring that authorized software, such as virus detection software, has been installed properly. This process assures that all active content applets have been adequately tested. This process also assures that compatible hardware and network protocols are being used.

Establishing Internet Links—Links that transfer a user's session from ITPO's intranet site to the web site of any outside entity are not permitted unless the approval of the Information Security manager has been obtained. Whenever these links are established, they must clearly notify the user that they are leaving the intranet and entering the Internet.

The company monitors and logs all Intranet accesses by individuals and reserves the right to access and report on this information.

8.0 SYSTEM ACCESS CONTROL POLICY

8.1 Objective

To control access to information;
To prevent unauthorized access to information system;
To detect unauthorized activities

8.2 Purpose

This policy addresses ITPO's intent to safeguard computing resources from various internal threats. This policy shall underline appropriate user etiquette for workstation usage and define procedures for safeguards.

8.3 Policies in detail

All ITPO computers that store sensitive information, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Systems department. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered. Multi-user systems throughout ITPO must employ automatic log off systems that automatically terminate a user's session after a defined period of inactivity.

8.4 Illegal Usage

Transmission, storage, or distribution of any information, data or material in violation of any applicable law or regulation is prohibited. This includes, but is not limited to: copyrighted material, trademark, trade secret or other intellectual property used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat.

8.5 Security

Violations of system or network security are prohibited, and may result in criminal and civil liability until unless they are authorized to do so. Examples include, but are not limited to the following: Unauthorized access, use, probe, or scan of a systems security or authentication measures, data or traffic; Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks; Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

8.6 Use of desktop systems

Employees are responsible for the security and integrity of information stored on personal desktop system. This responsibility includes making regular disk backups, controlling network access to the machine, and using virus protection software. Backups shall also include the backup of registry. Avoid storing passwords or other information that can be used to gain access to other network resources. Computer accounts, passwords, and other types of authorization are assigned to individual Employees and must not be shared with others. ITPO users are responsible for any such use of his/her account.

8.7 Logging off or locking the Workstation

ITPO users shall either log off or lock the workstation if they will be away from their desk any lengths of time. The workstation shall be configured to lock automatically using a secure screen saver if it is not used for a period of 5 minutes.

8.8 Personal Work

Computing facilities, services, and networks may not be used other than the work related with ITPO, which is given from time to time.

8.9 Unauthorized access

ITPO employees shall not:

- Damage computer systems

- Obtain extra resources which are not authorized to an individual
- Deprive another user of authorized resources
- Gain unauthorized access to systems

by using knowledge of:

- A special password
- Vulnerabilities in computer systems
- Another ITPO users password
- Access ability of ITPO used during a previous position

8.10 Resources Sharing

All the shares on the systems should be protected by password. All directories and sub-directories, which are shared, shall be protected by proper user authentication and permissions to access with relevant access rights.

8.11 Harmful activities

The harmful activities such as creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to equipment, software, applications, data belonging to ITPO or clients; and the like are strictly prohibited.

8.12 Use of privileged access

Special access to information or other special computing privileges is to be used during official duty only. Information that is available through special privileges is to be treated as private & confidential. A deliberate attempt to degrade the performance of a computer system or network or access to any restricted IT Infrastructure is prohibited.

8.13 Software Copyright and Licenses

- All software installed into individual machines must carry valid and appropriate license.
- Users should not copy the software from the network and install into other machines without obtaining appropriate licenses.

- Users should not distribute software (e.g. setting up ftp server) if they do not have the right to do so.
- Employees are not permitted to bring software from home or any other external source and load it on ITPO computers, unless specifically permitted in writing by the Information Systems Manager at CO and by Regional System in-charge at RO.
- Only IT support providers are authorized to load shareware and freeware software onto ITPO computers, after having ensured that software is virus free and written permission granted by Information Systems Manager at CO and by Regional System in-charge at RO.

8.14 Access Controls

- No default logins will be granted except for restricted reads approved by Information Systems Committee.
- Any visitor, guest and anonymous account to be deleted.
- No direct access to a database by a user will be permitted without permission from Information Systems Manager at CO.
- Users will not bring non-ITPO computer equipment into the ITPO network, unless specifically permitted in writing by the Information Systems Manager at Headquarters and by Regional Manager at RO.
- Users logon access to the network is restricted to the computers he / she normally uses.
- Administrative account will be permitted only direct / local logon to the server and not from the network, to unable any hacking from the network as administrator.
- Provide separate normal user account to the administrator for performance of non-administrative duties.
- No system administrator will keep his logon open indefinitely and will ensure that he necessarily logs off from the system at the end of his duty hours. Same rule will apply to users as well.

8.15 Access rights eligibility

- "Need based Approach" will be adopted for assigning access rights.

- Any significant changes in the role of a person will be accompanied with equal measure of changes in the person's access rights.
- For Operating System/ databases: System administrators will be granted access as per the need of their defined role.
- For Application Systems / ERP: Users will be granted access as per their functional need.

8.16 Access rights authority

Access rights would be granted as follows:

- For Operating System/ Databases: As per recommendations from HOD (Systems)/DGM/Senior Manager (Systems).
- For Application Systems / ERP: As per recommendations from HOD from concerned Division at Headquarters and Regional Manager at RO.

8.17 Formal review of Authority Matrix

- Quarterly by HOD (Systems)/DGM/Senior Manager (Systems) in case of OS and DBMS.
- Half Yearly by Data owners in case of Application Systems / ERP.

9.0 CLEAR DESK AND CLEAR SCREEN POLICY

9.1 Objective

To prevent compromise or theft of information and information processing facilities.

9.2 Purpose

Information and information processing facilities should be protected from disclosure to, modification of or theft by unauthorized persons and controls should be in place to minimize loss or damage.

9.3 Policies in detail

Organization should consider adopting a clear desk policy for papers and removable storage media and a clear screen policy for

information processing facilities in order to reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours. Unless information is in active use by authorized people, desks must be clear and clean during non-working hours to prevent unauthorized access to information. Officials must position their computer screens such that unauthorized people cannot look over their shoulder and see the sensitive information displayed.

The following controls should be considered:-

- Unless information is in active use by authorized personnel, desks must be absolutely clear and clean during non-working hours with all sensitive information or valuable data is properly secured or locked away.
- Sensitive information must always be locked in approved containers (ideally in a fire-resistant safe or cabinet) for sensitive information and must not be left unattended in any unsecured location.
- When not in use, sensitive information left in an unattended room must be locked away in appropriate containers.
- When not being used by authorized officials, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information and all computer media containing sensitive information must be locked in file cabinets, desks, safes, or other furniture.
- All officials who handle ITPO's secret, confidential, or private information must adequately conceal this information from unauthorized disclosure to nearby non-authorized parties.
- Personal computers and computer terminals and printers should not be left logged on when unattended and should be protected by key locks, passwords, screen savers or other appropriate controls when not in use. The use of screen savers or screen shields should be considered for computer monitors in open areas or where public may have oversight of the screen.
- All workstations located public areas have password-locked screen savers enabled to activate on either 15 minutes of inactivity.
- Scanners/ Photocopiers/fax machine/ printers should be locked or protected from unauthorised use in some other way outside normal working hours.

- Sensitive or classified information, when printed, should be cleared from printers immediately.

10.0 BACKUP POLICY

10.1 Objective

To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters;
To maintain the integrity and availability of information processing and communication services.

10.2 Purpose

Routine procedures should be established for carrying out the agreed back-up strategy taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment. In order to safeguard information and computing resources from various business and environmental threats, systems and procedures shall be developed and implemented for backup of all business data, related application systems and operating systems software. This shall be done on a scheduled basis and in a standardized manner across the organization.

10.3 Policies in detail

All personal computer software must be copied prior to its initial usage, and such copies must be stored in a secure location such as a locked file cabinet. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

10.4 Backup and Recovery Procedures

Back-up copies of essential business data and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business data and software could be recovered following a computer disaster or media failure. Back-up

arrangements for individual systems should meet the requirements of business continuity plans.

10.5 Backup Information

Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

10.6 Backup Media and Security

It shall be ensured by System Administrator that the media is regularly examined for readability of the data. The backup media shall be replaced immediately after encountering the error or at predefined time intervals whichever is earlier. The backup media shall be appropriately labeled and numbered. Backup media should be controlled and physically protected. Appropriate operating procedures should be established to protect tapes, disks, data cassettes, input/output data and system documentation from damage, theft, unauthorized access and virus attacks as appropriate.

11.0 LAPTOP SECURITY POLICY

11.1 Objective

To maintain the security of portable devices like laptops;
To reduce the disruption caused by theft or unauthorized information disclosure from a laptop.

11.2 Purpose

This policy ensures that the valuable data contained in Laptops is secured from theft and/or unauthorized access. This policy establishes requirements that should be met by all Laptop/Laptops computers used by employees of ITPO.

This policy shall be implemented to reduce the disruption caused by theft or unauthorized disclosure of information exist Laptops to an acceptable level through a combination of preventive controls.

11.3 Physical Security

- Employees using a Laptop shall ensure physically secure storage outside the office.
- All the Laptops should be under Insurance cover to protect against theft.
- They should be protected from environmental threats such as dust, excessive heat, and radiation with suitable measures such as using protective equipment.

11.4 Laptop Pool

Laptops, which are temporarily not used, shall be kept in a pool. The retrieval and issue of Laptop/Laptops must be documented along with details of users and the purpose of taking the Laptop/Laptops. When handing over to a user, sufficient charging of the batteries must be ensured.

11.5 Laptop Protection

Each Laptop owned by ITPO shall be provided with boot password protection. Passwords shall be changed before handing over Laptop to the user and records shall be maintained. If the Laptop is handed over to another employee of ITPO, its password shall be altered. All the Laptops shall be enabled with the power save option, which can be activated by a specific key combination. If Laptop is not used for a longer break, it should be switched off.

11.6 Change Management

When the user of a Laptop PC changes, it shall be ensured that no sensitive data of the organization or computer viruses are present on the system. The operating system and other software shall be freshly installed and configured.

11.7 System Security

All the Laptops should be installed with Anti-Virus Software as referred in the Anti-Virus Policy. Users shall not create universally accessible shares in the Laptops. All departmental IT equipment

used outside the department's premises should be subject to the same degree of security as that afforded to equipment used for the same activities on-site. Passwords should never be passed 'in the clear'.

11.8 Data Backup

All the data on the Laptop shall be backed up and kept in a safe place before any travel. Regular manual backups shall be made of the data on the Laptop as per Backup Policy.

12.0 INCIDENT MANAGEMENT POLICY

12.1 Objective

To minimize the damage from security incidents and malfunctions; and
To monitor and learn from such incidents.

12.2 Purpose

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and reduce the cost associated with security incidents

12.3 What is an 'Incident'?

'Incident' is a term related to exceptional situations or a situation that warrants intervention of specialist help or senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of the company. An incident may relate to any of the following:

- Suspected hacking attempts
- Successful hacking attempts
- Hardware resources and components lost / stolen

- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Failure / crash of IT equipment
- Power problems
- Natural calamity or disaster

12.4 Detecting or Reporting initial Incidents

An incident may be detected by anybody in the organization. The concerned personnel shall immediately bring it to the notice of the Incident Response Team or Systems Manager concerned.

12.5 Incident categorization

An incident should be categorized into various severity levels. These severity levels are based on the impact to ITPO and can be expressed in terms of financial impact, credibility impact, impact to sales and marketing, impact to ITPO's image or impact to trust by ITPO's customers.

12.5.1 Level One Type Incident

A small-scale response, involving one of the support services within the organization and external intervention is not required. The resident engineer / system official / AMC Provider should be able to resolve the incident.

12.5.2 Level Two Type Incident

A significant response is required by multiple services within the organization and external emergency services may also be involved. E.g. Theft. Respective functional Senior Manager/Manager or System Administrator or System official at RO is required to manage the immediate response.

12.5.3 Level Three Type Incident

A major community response is required, where the external emergency services assume the overall management of the incident, in conjunction with Organization services. E.g. Fire. External experts like various service providers may be called in for help.

HOD Headquarters has to declare the level of the incident.

12.6 Investigation Incidents

Incident Response Team / System official must identify the cause for Incident, collect evidences and appraise its impact on ITPO's Systems and data. Incident Response team considers the following while identifying the causes of Incidents:

- Evidences for security breaches are collected if Incident causes a breach with statutory, regulatory or contractual obligations, criminal or civil law
- Evidences collected have to be evaluated according to their particular circumstances, and this may, or may not, require various departments to be involved

12.7 Incident Recovery Action Plan

HOD Headquarters and Incident Response Team, in consultation with respective department management(s) shall prepare the corrective action plan for the incident. The action plan, though specific to each case, shall typically cover the following:

- Particulars about the operating unit, location, date and time etc
- Facts and explanation / reasons for the incident
- Other business units affected
- Corrective action to be taken
- Estimated cost of implementing the corrective action
- Estimated time frame, start date and end date
- Personnel responsible for taking the action

12.8 Documentation and Reporting

The Incident Response Team will analyze the impact of the incident, then frame a detailed report and send it to the System in-charge at CO / Regional in-charge at RO.

The same shall be formally documented along with relevant evidence collected or observations

12.9 Incidences due to violation of Security Policies

Incidence arising out of violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process. The disciplinary actions will be as envisaged by ITPO's rules and regulations.