INDIAN PORTS ASSOCIATION

Information Technology (IT) Policy for Hardware, Software and other Accessories

ICT Department
January 2020

Table of Content

Information Technology (IT) Policy
for Hardware, Software and Accessories

Indian Ports Association (IPA) was constituted in 1966 under Societies Registration Act, primarily with the idea of fostering growth and development of all Major Ports which are under the supervisory control of Ministry of Shipping. Over the years, IPA has consolidated its activities and grown strength by strength and considered to be a think tank for the Major Ports with the ultimate goal of integrating the maritime sector.

Introduction:

IPA provides IT infrastructure to its employees to enhance their efficiency and productivity. These infrastructures are meant as tools to access and process information related to their areas of work. These infrastructures help IPA officials to remain well informed and carry out their functions in an efficient and effective manner. For the purpose of this policy, the term ‘IT infrastructure’ includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

Misuse of these infrastructures can result in unwanted risk and liabilities for the IPA. It is, therefore, expected that these infrastructures are used primarily for IPA related purposes and in a lawful and ethical way.

Scope:

This policy governs the usage of IT infrastructures from an end user’s perspective. This policy is applicable to all employees of IPA.

Objective:

The objective of this policy is to ensure proper access to and usage of IPA IT infrastructure and prevent their misuse by the users. Use of infrastructures provided by IPA implies the user's agreement to be governed by this policy. The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy. This document is prepared with the reference from Policy on Use of IT Resources of Government of India, Ministry of Communications and Information Technology and email policy MeitY.

Categories of Employees:

The following levels of employees are in IPA as mentioned in the RSP:

- Director level
- HoD level
- Officer level – Class I & Class II
- Staff level – Class III & Class IV

Type of Employment

- Permanent
- Contract
  - Direct contract /consultant
  - Third party contract

1. Desktop / Laptop Devices Policy:

Desktops shall normally be used only for transacting IPA office work. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

Security and Proprietary Information:

- User shall take prior approval from the competent authority of IPA to connect any access device to the network.
- All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
- Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

- Users shall properly shut down the systems before leaving the office.
- User should not store the sensitive data on the desktop connected to the internet.
- Booting from removable media shall be disabled. Use of external storage media by user shall not be allowed. If the use of external storage is necessary, with due approval from the competent authority, the port will be opened.
- Users shall be given an account with limited privileges on the client systems. User shall not be given administrator privileges.
- If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be disconnected from the network immediately and reported to the ICT department immediately for corrective action.

Use of software on Desktop systems:

- Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
- All the software officially installed shall be the authorized/ licensed versions and there shall be no pirated versions.
- A list of allowed software shall be made available by the ICT department. Apart from the Software mentioned in the list, no other software will be installed on the client systems.
- Any additional software need to be installed, then user should take prior approval from the competent authority.

Purchase of Desktop & laptop:

The desktop computer must be purchased as standard desktop brand and must be from the Original Equipment Manufacturer listed in the Gartner list {such as HP, Dell, Lenovo, Apple, Acer etc.}.

The minimum desktop specification details are as follows:

Details	**Category 1**	**Category 2**	**Category 3**	**Category 4**
Processor Speed	8th Gen i7	8th Gen i5	8th Gen i3	7th Gen i7
RAM	8 GB	8 GB	4 GB	4 GB
Hard Disk	1 TB	1 TB	500 GB	500 GB
Operating System	Win 10	Win 10/8.1	Win 10/8.1	Win 10/8.1

Any change from the above requirements must be approval by the competent authority.

The laptop must be purchased from the Original Equipment Manufacturer listed in the Gartner list {such as HP, Dell, Lenovo, Apple, Acer etc.}.

The minimum laptop specification details are as follows:

Details	**Category 1**	**Category 2**
Processor Speed	8th Gen core i7	8th Gen core i3
RAM	8 GB	8 GB
Hard Disk	1 TB	1 TB
Operating System	Win 10	Win 10/8.1
Weight	Less than 1.5 Kg	Less than 2 Kg

Any change from the above requirements must be approval by the competent authority.

Purchase of computer peripherals:

Computer system peripherals are add-on devices such as printers, scanners, external hard drives etc. Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals. The peripherals purchased must be compatible with all other computer hardware and software and All purchases of computer peripherals must be supported by guarantee and/or warranty.

All purchases of desktops, laptops and computer peripherals should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers and other peripherals would be maintained by AMC vendor / agency with the support of external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

The purchase of all computer related items to be compatible with the IPA requirement and it will be in line with the Procurement Manual and Financial policies.

Power Connection to Computers and Peripherals:

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring**.**

Purchase of Server systems:

Server systems can only be purchased by with the clear recommendation of Head of Department, ICTD. The Server systems purchased must be compatible with all other computer hardware in the organisation.

All purchases of server systems must be supported by guarantee and/or warranty and be compatible with the IPA requirement and it will be in line with the Procurement Manual and Financial policies.

IT Hardware Failure:

Where there is failure of any of the hardware, this must be referred to IT Associate (Hardware) immediately. It is the responsibility of IT Associate (Hardware) to assess the primary troubleshooting in the event of IT hardware failure, if the problem exist the AMC vendor will take-up the issue. A register is maintained for the complaint and resolve.

2. Password Policy:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change of the passwords.

All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords. Password shall be enforced to be of a minimum length of 8 character and comprising of mix of alphabets, numbers and characters.

Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them. Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.

Suggestions for choosing passwords: Passwords may be chosen such that they are difficult-to-guess yet easy-to-remember.

- String together several words to form a pass-phrase as a password.
- Combine punctuation and/or numbers with a regular word.
- Bump characters in a word a certain number of letters up or down the alphabet.
- Shift a word up, down, left or right one row on the keyboard.

Compliance:

- Personnel authorized as Internal Auditors shall periodically review the adequacy of such controls and their compliance.
- Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

3. Security Policy:

The policy provides guidelines for the protection and use of information technology assets and resources within the IPA to ensure integrity, confidentiality and availability of data and assets.

For all hardware products like desktops, servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through passwords, keypad, lock etc.

All technology that has internet access must have anti-virus software installed. It is the responsibility of IT department to install anti-virus software and ensure that this software remains up to date on all technology used by the IPA.

Keeping device secured:

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Cyber Security Policy for Cloud based systems/application like PCS, Port EBS, Unnati, etc to be prepared under the guidance of National Critical Information Infrastructure Protection Centre (NCIIPC) and Indian Computer Emergency Response Team (CERT-IN).

4. Antivirus Policy:

Computer viruses are data destructive programs written with the intent of copying and spreading the destruction to other computers and programs.

Symptoms of an Infected Computer:

The following are common symptoms of a computer infected with a virus:

1. The computer fails to start
2. Programs will not launch or they fail when simple commands are performed
3. Names of files are changing or become unreadable
4. File contents change or are no longer accessible
5. Unusual words or graphics appear on the screen
6. Hard or floppy disks are formatted
7. Variations occur in computer performance, such as slowing down in loading or operation

Deployment of Antivirus:

1. For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed.
2. In a networked environment, an antivirus server should be deployed and all the workstations should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as updation of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.
3. Identify all the possible entry points in the network through which a virus attack is possible and all the traffic entering the network through these points should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP or POP3.

The suggested best practices for keeping PC's free from a possible virus attack.

1. A good anti-virus product should be chosen for the organization. A centralized server based antivirus system is suggested for an organization with a computer network.
2. For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
3. For a networked environment there must be a central server to check for viruses' in all the machines automatically.
4. The following schedule is suggested for a full scan of the PC's.
   a. Servers: Daily
   b. Workstations: Daily

   Schedule the operation when there is least human interaction with the work stations.
5. The antivirus software should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.

7. External media (ex. Floppy, CD’s) is one of the most potent medium for transmission of viruses’, hence it must not be used in the network except for a few pre-determined PC’s approved by competent Authority.

8. Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies of the organization.

9. Unneeded services should be turned off and removed. By default many operating systems install auxiliary services that are not critical e.g. an FTP, telnet or a web server. These services are avenues to attack, these services to be stopped.

10. Enforce a password policy. Complex password makes it difficult to crack password files on compromised systems/computers.

11. Mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block/ remove attachments that are commonly used to spread viruses, i.e, .vbs, .bat, .exe, .pif, & .scr files.

12. Employees must be trained not to open attachments unless they are expecting them.

16. Do not allow user to execute software downloaded from internet unless certified safe by system administrator.

17. In the case of a virus attack the following steps are required to be taken.

a. The network share of the machine has to be stopped

b. The contact person for cleaning the machine of virus has to be notified

c. There must be a mechanism where an authorised expert/work station is notified automatically in case of a virus attack.

5. Access to the Network (Internet and Intranet):

The user will be provided with internet through LAN as per the below specified.

Filtering and blocking of sites:

IPA may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network. IPA may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the productivity of the users.

Access to Wireless Networks:

To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

Employees when using IPA wireless network access in their device, the user should register with ICTD department with the approval of competent authority. The ICT department will maintain a register on the usage of wireless internet and its accessibility. IT Associate (Hardware) is the responsible for maintain the wireless network, Register, primary troubleshooting, to access to guest, etc.

6. E-mail Policy:

The objective of this policy is to ensure secure access and usage of e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful and ethical manner.

Users shall not download e-mails from their official e-mail account, configured on the Government of India mail server, by configuring POP or IMAP. If user required to download through POP or IMAP, then user should take prior approval from the competent authority.

Auto-save of password in the Government e-mail service shall not be permitted due to security reasons.

No private email accounts (Gmail, Yahoo, Rediff, Hotmail, etc) are used for official communication, this should be strictly followed by the users.

7. Website Policy:

The purpose of this policy is to provide guidelines for the maintenance of all relevant technology issues related to the website.

A register to be maintained with all domain names, date of created, list of hosting service providers, etc. Keeping update of the register is the responsibility of IT department.

All content on the IPA website is to be accurate, appropriate and current. This will be the responsibility of IT department. Before uploading any content /data/photo/video, etc there should be clear approval from the competent authority.

Website Disruption:

In the event that IPA website (like Official website, PCS portal, Maritime Portal, etc) is disrupted, the following actions must be immediately undertaken by the IT Associate (Software) with the HoD guidance:

- Website host to be notified
- ED(IT) & AD(IT) must be notified immediately

8. Software Policy:

This policy provides guidelines for the purchase of software for the IPA to ensure that all software used by the IPA is appropriate, value for money and where applicable integrates with other technology. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

All software's like licensed, open source, freeware, etc. must be approved by competent authority prior to the use or purchase or download of such software.

All license software must be purchased in the name of IPA. License products like Operating System, Microsoft Office, Convertor software, Database software, etc will be installed for the users and Open source/ free ware products like Acrobat Reader, Win RAR, etc will be installed for all users.

9. External / Own device Policy:

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets, etc for IPA purposes. All staff who use or access IPAs technology equipment and/or services are bound by the conditions of this Policy.

Employees when using personal devices for IPA use should register the device with ICTD department with the approval of competent authority.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer IPA or personal sensitive information to the device. Sensitive information includes personal information that you consider sensitive to the IPA, employee details, reports & statistical data, intellectual property, etc.}

- Not to use the registered mobile device as the sole repository for IPA information. All information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that IPA information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
- Not to share the device with other individuals to protect the IPA data access through the device
- To abide by IPA internet policy for appropriate use and access of internet sites etc.
- To notify IPA immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to IPA equipment.
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data.

10. Backup Policy:

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into many volumes typically C, D and so on. OS and other software should be on C drive and user’s data files on the other drives (e.g. D, E). In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data on CD / DVD or other storage devices such as pen drives, external hard drives.

Auto backup session will be enable in the Active Directory System within the network.

Eligibility:

Levels	**Desktop**	**Laptop**	**Tablets / iPAD**	**Internet** (Data card/ dongle)	**Pen drive/ External storage**	**Printer & Scanner**	**Video Conference & IP Phone**
Director level							
Chairman, Vice Chairman & Managing Director	All in One	Weight less laptop	Yes	Yes	Pen Drive & External HDD	MFP	Yes
Executive Director	All in One	Weight less laptop	Yes	Yes	Pen Drive & External HDD	MFP	Only IP Phone
HoD Level							
Chief Administrative Officer, Chief Informatics Officer & Head of Statistical, consultancy dept.	High end Desktop	High end laptop	Only Tab	Yes	Pen Drive & External HDD	MFP	Only IP Phone
Officer Level							
Joint Director, Sr. Deputy Director, Deputy Director & Deputy Manager	Yes	Yes	NA	Yes	Yes	Printer cum scanner	Only IP Phone
Assistant Director, Assistant Manager, Consultant & Specialist	Yes	Yes	NA	Yes	Yes	Printer cum scanner	NA
Staff level							
Executive Assistant, Sr. Assistant, Supervisor, Assistant & Associate	Yes	NA	NA	NA	Yes	Only printer	NA
Jr. Assistant, Receptionist, Data entry operator	Yes	NA	NA	NA	Yes	Only printer	NA

Cost Ceiling: (Rs. In lakhs)

Levels	Desktop	Laptop	Tablets / iPAD	Internet (Data card/ dongle)	Pen drive/ External storage	Printer & Scanner	VC & IP Phone
Director level							
Chairman, Vice Chairman & Managing Director	1.5	2.0	0.40 to 0.50	unlimited	0.20	0.80 to 1.00	2.0 to 3.0
Executive Director	1.0	1.50	0.30 to 0.40	unlimited	0.10	0.70 to 0.80	1.0
HoD Level							
Chief Administrative Officer, Chief Informatics Officer & Head of Statistical, consultancy dept.	0.60 to 0.70	0.80 to 1.0	0.10 to 0.20	unlimited	0.07	0.50 to 0.60	1.0
Officer Level							
Joint Director, Sr. Deputy Director, Deputy Director & Deputy Manager	0.55 to 0.65	0.75 to 0.80	NA	unlimited	0.05	0.50 to 0.60	1.0
Assistant Director, Assistant Manager, Consultant & Specialist	0.50 to 0.55	0.60 to 0.70	NA	unlimited	0.05	0.20 to 0.30	NA
Staff level							
Executive Assistant, Sr. Assistant, Supervisor, Assistant & Associate	0.45 to 0.50	NA	NA	NA	0.005	0.08 to 0.10	NA
Jr. Assistant, Receptionist, Data entry operator	0.45 to 0.50	NA	NA	NA	0.005	0.06 to 0.08	NA

Responsibility:

- Any Hardware, Network and Software related issue first level contact: Junior / Executive Assistant (EDP).
- Any Hardware, Network and Software related issue Second level contact: Assistant Director (IT).
- Overall Responsible: CIO, ICTD
- Review and Recommending Officer: ED, IPA
- Competent Authority: Chairman, Vice Chairman & Managing Director.

General Guideline:

- The entire desktops / laptops of IPA are login through Active Directory System.
- Latest version of Office, Acrobat, Win Rar, etc will be preloaded in the system.
- Every year in the month of February, the IT policy should be updated with latest technology and placed to competent authority for approval & implementation.
- Every week Friday in the first half is a day for data backup by individual users.
- Internet are provided to all users as per the firewall policy.
- Updation of website content/ Gallery/ documents, etc should be done, based on the approval from the competent authority.
- All hardware accessories should be at least one-year warranty from the date of purchase / date of installation.
- Computer & other accessories should be under AMC with the respective OEM.
- Every quarter preventive maintenance should be done for desktop, printer, etc.
- A separate register should be maintained for recording all the AMC validity period with escalation matrix, Internet service provider escalation matrix, etc.

11. Online Procurement policy:

An online marketplace (or e-commerce marketplace) is a type of e-commerce site where product or services are offered by a number of sellers and all the buyers can select the product/ services offered by any one of the seller, based on his own criteria.

In an online marketplace, Purchaser’s transactions are processed by the marketplace operator and then product/services are delivered and fulfilled directly by the participating retailers. Other capabilities like catalogues, ordering, posting of requirements by Purchasers, Payment gateways etc.

In general, because online marketplaces aggregate products from a wide array of providers, selection is usually wider, availability is higher, and prices are more competitive than in vendor-specific online retail stores.

DGS&D has developed an online Government e-Market Place for common use goods and services. The procurement process on GeM is end to end from placement of supply order to payment to suppliers. This is to ensure better transparency and higher efficiency. All the process will be electronic and online. The Procurement of Goods and Services by Ministries or Departments will be mandatory for Goods or Services available on GeM.

The GeM portal shall be utilized by the Government buyers for direct on-line purchases as under: -

- Up to Rs. 50,000/- (Rupees Fifty thousand) through any of the available suppliers on the GeM, meeting the requisite quality, specification and delivery period.
- Above Rs. 50,000/- (Rupees Fifty thousand) through the GeM Seller having lowest price amongst the available sellers, of at least three different manufacturers, on GeM, meeting the requisite quality, specification and delivery period.

For the purchase of any IT related accessories through online, then it is recommended to purchase through GeM portal. The Products of computer peripherals which are not available in GeM online portal and it is available in other portal like Amazon, Flipkart, etc the same shall be purchase with the approval of competent Authority. While purchasing through the products through online portal, ensure the Warranty /Guarantee. The payment shall be made by Payment gateways.

The online procurement policy should be in line with the Procurement Manual and Financial policies.

Version Control:

Version No	**Date**	**Prepared by**	**Pre Reviewed by**	**Final Reviewed by**	**Approved by**
1.0	03.07.2018	Assistant Director (IT)	Chief Informatics Officer	Executive Director	Managing Director
1.1	17.07.2018	Assistant Director (IT)	Chief Informatics Officer	Executive Director	Managing Director
1.2	25.03.2019	Assistant Director (IT)	Chief Informatics Officer	Executive Director	Managing Director
2.0	10.01.2020	Assistant Director (IT)		Executive Director	Managing Director