

# **INDOCO REMEDIES LIMITED**

## **I.T. POLICY**

**(Version 1.0)**

**(Effective From : 01/07/2018)**

## TABLE OF CONTENTS

01. POLICY STATEMENT	3
02. VIRUS PROTECTION	4
03. ACCESS CONTROL	5
04. PEN DRIVES CD DRIVES AND OTHER READ / WRITE AND STORAGE DEVICES.	6
05. SHIFTING OF SYSTEMS	7
06. INSTALLATION AND REINSTALLATION	7
07. INVENTORY MANAGEMENT – SOFTWARE / LICENSES	7
08. LAN SECURITY	9
09. SERVER SECURITY	10
10. WINDOWS SECURITY	10
11. WIDE AREA NETWORK SECURITY	11
12. TCP/IP & INTERNET SECURITY	11
13. USAGE OF INTERNET / E-MAIL	11
14. BACKUP / RESTORE PROCEDURE	13
15. I.T. PROCUREMENT - SYSTEM	16
16. I.T. PROCUREMENT - INTERNET / MPLS-VPN / STORAGE	20
17. REPLACEMENT OF SYSTEM	21
18. I.T. SYSTEM – DAMAGES AND RECOVERY	21
19. DISPOSAL OF SYSTEM	22
20. ARCHIVAL OF WEBSITE INFORMATION	22
21. POLICY REVIEW	23

## 1.0 POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate Protection and confidentiality of all corporate data and proprietary software Systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized persons, and to ensure the integrity of all data and configuration Controls. This policy is applicable to Indoco Remedies Ltd and its subsidiaries."

### Summary of Main Security Policies.

- 1.1 Confidentiality of all data is to be maintained through limited access and Mandatory access controls.
- 1.2 Internet and e-mail facility is restricted to authorized Personnel only and is permitted only through written / electronic approval of site head.
- 1.3 Only authorized and licensed software may be installed, and Installation may only be performed by I.T. Department staff or by external agencies through proper authorizations and prior intimation to the respective IT department head. The use of unauthorized software is prohibited. In the event of any unauthorized software being discovered it will be removed from the Workstation immediately and further action will be taken on the concerned user.
- 1.4 Data may only be transferred for the purposes determined in the Organization's requirement needs. All disks / drives and removable media from external sources must be Virus checked before they are used within the Organization. It may be only brought into the facility by intimating the IT HOD and with approvals from user HOD.
- 1.5 All External Ports like USB, Blue Tooth will be blocked (except where it is required to connect to computer devices like monitor, mouse and printers) as per the IT policy except in the case of eligible laptop holders and IT personnel who have been approved by respective HODs or Management.
- 1.6 Passwords must consist of a mixture of at least 8 alphanumeric Characters, and must be changed every 45 days and must be unique.
- 1.7 Passwords for each user should not be shared with others and the concerned user is responsible for all data generated or modified using the respective user ID. Hence any changes made using the specific ID is the responsibility of the person to whom the ID has been assigned.
- 1.8 Workstation configuration may only be changed by I.T. Department Staff and

maintaining proper inventory documentation.

- 1.9 To prevent the loss of data, backup of data and application has to be taken as per the process defined below.

## **2.0 Virus Protection**

- 2.1 The I.T. Department will have virus scanning Software for scanning and removal of suspected viruses.
- 2.2 Corporate file-servers and workstations will be protected with virus scanning software.
- 2.3 All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.
- 2.4 No data or any kind of media can be brought into the organization. If permitted, by authorized persons, the data on such media needs to be compulsorily scanned for viruses.
- 2.5 As far as possible, all demonstrations by vendors will be run on their machines and not the Organization's. If permitted, the software media from where it is loaded should be scanned and after completion of presentation, the same should be removed from the installed location.
- 2.6 Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
- 2.7 To enable data to be recovered in the event of a virus out-break, regular backups will be taken by the I.T. Department as per the laid down procedures.
- 2.8 Management strongly endorses the Organization's anti-virus policies and will make the necessary resources available to implement them.
- 2.9 Users will be kept informed of current procedures and policies related to antivirus.
- 2.10 Users will be notified of virus incidents.
- 2.11 Employees will be accountable for any breaches of the Organization's Anti-virus policies whether deliberate or otherwise, after thorough investigation.
- 2.12 Anti-virus policies and procedures will be reviewed periodically.
- 2.13 In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread through the network.
- 2.14 Users should not download any freeware or non-official data.

### **3.0 Access Control**

- 3.1 Users will only be given sufficient rights to particular systems to enable them to perform their job function. User rights will be kept to a minimum at all times and need to be authorized in writing/ electronically by concerned HOD, before the same is assigned.
- 3.2 Users requiring access to certain systems must make a written application on the forms provided by the I.T Department and get it authorized as per laid down procedures- User Request Format.
- 3.3 Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end- user department.  
The system administrator will be responsible for the maintaining the integrity of the end-user department's data and for creation of users and assigning the end-user access rights based on the recommendations of head of end user departments.
- 3.4 Physical / electronic access to the network/servers and systems will be by individual username and password or by smartcard and PIN number / biometric.
- 3.5 Usernames and passwords must not be shared by users among themselves.
- 3.6 Usernames and passwords should not be written down.
- 3.7 Usernames will consist of initials or names and surnames or sections in the case of group access.
- 3.8 All users will have an alphanumeric password of at least 8 characters. This may be relaxed depending on the inherent properties of the system.
- 3.9 Passwords will expire every 45 days.
- 3.10 Intruder detection will be implemented where ever possible. The user account will be locked after minimum 3 incorrect attempts as per policy applicable and feasibility.
- 3.11 The concerned I.T. Department will be notified in writing or electronically of all employees leaving the Organisation's employment by the HR department. The I.T. Department will then remove the employee's rights to all systems.
- 3.12 All network/server ADMINISTRATOR passwords and system ADMINISTRATOR passwords will be stored in a secure location in case of an emergency or disaster, for example a fire proof safe in the I.T. Department as per the laid down procedures.
- 3.13 Auditing will be implemented on all systems to record login attempts / failures, successful logins and changes made to all systems.
- 3.14 I.T. Department staff will not login as ADMINISTRATOR on windows systems but will use the administrator equivalent ID to perform administrator functions.
- 3.15 Use of Administrator username on Windows is to be kept to a minimum.

- 3.16 Default passwords on systems such as Oracle and SQLServer must be changed after installation
- 3.17 Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in Writing on the forms provided by the I.T. Department.
- 3.18 File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.  

No user should store data on the local machine so as to ensure that important data is not saved on the drive thus ensuring that the data does not get lost in case of a system failure. In case of Laptop user, it is the user responsibility to store data on the network server.
- 3.19 As far as possible the administrator should ensure that deletion or modification of data generated by software systems and data acquisition systems is not possible by ordinary users. Renaming of files and folders should also be restricted.
- 3.20 Using computer resources to access the information or for personal purposes, without approval from the user's HOD and the IT department, may be considered as a cause for disciplinary action.
- 3.21 All user access rights /profile will be properly documented and maintained by IT.

#### **4.0 Pen drives, CD Drives and other read / write and storage devices.**

- 4.1 Usage of pen drives, CDs, flash drives and all such devices is not allowed and hence disabled on all computer system. This facility is available only to IT department for official purpose to transfer data from one device / location to the other and to help other users to use such features as may be required. This facility is also available for eligible employees who have been provided laptops by the company under the company policy schemes and approved by respective HODs or Management.
- 4.2 For the purpose of transfer of any official data as per requirement, the device has first to be scanned by IT department for any virus related issues and then only such data can be transferred to the computer system as required once the device is clean.
- 4.3 No data should be copied onto the CD, pendrive or similar device unless duly authorized by the site head or department head.
- 4.4 All software / installation CDs which are to be used at the site has to be properly labeled and stored in a secure place in IT department.

- 4.5 Issue of media for installation etc. has to be maintained as a record and return of the same for storage has also to be recorded.
- 4.6 Similarly any new CDs received from supplier for any new system being used at the site has to be handed over to IT department after receipt and installation. Record of the new CD has also to be maintained.
- 4.7 IT department should keep track of all approvals regarding usage of USB storage.

## **5.0 Shifting of Systems**

- 5.1 Shifting of computer systems or any peripheral device or part of a computer system cannot be carried out by any employee or department and must be done only by IT personnel or under their supervision.
- 5.2 The movement can be carried out, in the absence of IT personnel only if the requirement is critical and after informing the concerned IT personnel.
- 5.3 Any change in the configuration of the computer system has to be approved by IT with a change request from the concerned HOD stating details of change and sufficient reason for the same.
- 5.4 No change or upgrade in the system, whether software or hardware should be made without proper authorization and documentation. This includes RAM upgrades or replacement of any computer part / installation of patches / changes in firmware.
- 5.5 All computerized systems falling under the purview of GMP related systems will by default fall under the scope of change control as per the laid down GMP procedures.
- 5.6 IT department should maintain records of the systems shifted

## **6.0 Installation & reinstallation**

- 6.1 After installation of new systems, necessary documentation has to be generated showing the location / site of installation and all other relevant details of the computerized systems.
- 6.2 No system within the plant, whether software or hardware is to be moved or re-installed without first documenting the movement sufficiently along with necessary approvals from concerned HOD and IT department. IT dept should maintain the proper records of the same.

## 7.0 Inventory Management – Software / Licenses

- 7.1 The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.
- 7.2 Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.
- 7.3 In case of replacement of systems, the original system being replaced should be returned and the IT department who would assess its usability and decide on the future use of the system.
- 7.4 All Software licenses procured will be managed centrally at HO I.T.
- 7.5 I.T department will be using License Management tool to manage compliances with respect to all software licenses.
- 7.6 Procurement of Licenses will be based on requirement and need basis. License procurement will be done twice in a year.
- 7.7 All Local IT at locations will send quarterly report of the network security & half yearly report of IT assets inventory & license utilisation
- 7.8 In-house developed software -

- All In-house developed software will be owned by Indoco Remedies Ltd and replication / duplication of the same by any individual is prohibited.
- Any In-house software development will be carried out on the test environment and after successful testing the new versions will be released on the Production /Live server.
- Source code of all In-house developed software will be backed up on a CD and the same will be backed up the network drive in a separate folder for In-house software backups. This will be further backed up as per the backup policy defined
- All In-house software should be properly documented along with user manual, process flow and installation manual.
- Any new requirement / upgrades in the existing software should be raised using the IT Change request format and proper justification by the user and approved by the HOD and Head of related departments. IT will then evaluate the requirement and take necessary action to incorporate the changes wherever possible / required.



## 7.9 External software –

- All Third party software which involves Indoco database will be procured only after signing an Non-disclosure agreement with the software provider.
- Any Third party software procurement will not be carried out without final approval from IT.
- IT will evaluate the requirement along with all related department and carry out feasibility study to analyze the software impact in the Indoco environment.
- All Third party software should have Installation manual, User manual and Installation modules.

## 8.0 LAN Security

### Switches

- 8.1 LAN equipment, bridges, repeaters, routers, switches will be kept in secure server rooms. Server rooms will be kept locked at all times. Access to server rooms will be restricted to I.T. Department staff only. Other staff and contractors requiring access to server rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.

### Workstations

- 8.2 Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows workstations may be locked.
- 8.3 All unused workstations must be switched off outside working hours.

### Wiring

- 8.4 All unused network points will be de-activated when not in use.
- 8.5 Users must not place or store any item on top of network cabling.
- 8.6 Redundant cabling schemes will be used where possible.

### Servers

- 8.7 All servers will be kept securely under lock and key.
- 8.8 Access to the system console and server disk/tape drives will be restricted to authorized I.T. Department staff only.

### Electrical Security

- 8.9 All computers, servers, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.
- 8.10 In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the generator takes over wherever generator is available.
- 8.11 In case of total power failure, IT department will shut down the servers and network.
- 8.12 All UPS's will be tested periodically.

### **9.0 Server Security**

This section applies to Windows & other work stations.

- 9.1 The operating system will be kept up to date and patched on a regular basis.
- 9.2 Servers will be checked regularly for viruses.
- 9.3 Servers will be locked in a secure room.
- 9.4 Where appropriate, the server console feature will be activated.
- 9.5 Remote management passwords will be different to the Admin/Administrator password.
- 9.6 Users possessing Admin/Administrator rights will be limited to trained members of the I.T. Department staff only.
- 9.7 Use of the Admin/Administrator/root accounts will be kept to a minimum.
- 9.8 Users access to data and applications will be limited by the access control features.
- 9.9 The system auditing facilities will be enabled.

### **10.0 Windows Security**

- 10.1 Windows Active directory policy is enabled
- 10.2 Administrator Use will be kept to a minimum.
- 10.3 All Windows & Mac System will be password protected.
- 10.4 Remote login facilities will be restricted to authorized I.T. Department staff only.
- 10.5 Telnet facilities will be restricted to authorized users.
- 10.6 Users access to data and applications will be limited by the access control features.

## **11.0 Wide Area Network Security**

- 11.1 Wireless LAN's will make use of the most secure encryption and authentication facilities available.
- 11.2 Users will not install their own wireless equipment under any circumstances.
- 11.3 Modems will only be used where necessary, in normal circumstances all communications should pass through the Organisation's router and firewall.
- 11.4 Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.
- 11.5 All bridges, routers and gateways will be kept locked up in secure areas.
- 11.6 Unnecessary protocols will be removed from routers.
- 11.7 The preferred method of connection to outside Organizations is by a secure VPN connection, using IPSEC or SSL.
- 11.8 All connections made to the Organization's network by outside organizations will be logged.

## **12.0 TCP/IP & Internet Security**

- 12.1 Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
- 12.2 Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
- 12.3 Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.
- 12.4 Network equipment will be configured to close inactive sessions.
- 12.5 Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.
- 12.6 Workstation access to the Internet will be via the Organisation's proxy server and website content scanner
- 12.7 All incoming e-mail will be scanned by the Organisation's e-mail content scanner.

## **13.0 Usage of Internet / e-mail (personal mails, mail sizes & external mail)**

- 13.1 Internet is a paid resource and therefore shall be used only for business work.
- 13.2 Indoco E-mail / Internet services should be available for official purposes only. Usage of external e-mail services like Gmail, Yahoo etc are strictly prohibited.
- 13.3 No personal emails should be sent / internet should not be accessed for personal use.

- 13.4 E-mail ID is to be provided to users only if it is approved by the concerned users superior or department head; in case of manufacturing facilities, by the site head / operations head. Final approval and creation of E-mail ID will be done by HR Dept.
- 13.5 There is a limit to the number of licenses available and hence all requests / sanctions of e-mail IDs should be done judiciously.
- 13.6 Access to external mail facility will be provided after proper approval / sanction from the department / sectional head/ site head. Final approval of the same in case of Plants will be given by Operations Head.
- 13.7 E-mails more than 10MB in size is restricted and cannot be sent by any user. Official attachments exceeding 7MB in size can be routed / uploaded through the FTP site / internet after proper approval from the HOD with the help of IT department.
- 13.8 A maximum of 25 recipients can be used in each mail sent. If there are more recipients, then multiple emails have to be sent.
- 13.9 Official mails / any other documents should not be sent to any other personal ID unless authorized and only when access through such external e-mail ID is required.
- 13.10 If there is a requirement for auto-forwarding of mails written permission from the HOD is required to allow the same.
- 13.11 Sending SPAM, including the transmission of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type are prohibited.
- 13.12 Internet facility is restricted to certain users only. Access to pornographic sites / material over the internet should be restricted through the firewall.
- 13.13 Any breach of this rule should be brought to the notice of HOD / higher up and strict action is to be taken against such violators.
- 13.14 Internet access shall be provided on "need to use" basis. Anyone who requires it shall be given access after appropriate authorization. Such users who need to access the internet officially, must put a request through the respective HOD and access can be provided by IT after IT receives the mail from respective HOD
- 13.15 Departments like accounts/ H.R. and purchase can be given restricted access to certain sites for statutory requirements by controlling the access on the firewall.
- 13.16 The company reserves every right to monitor, examine, block or delete any/all incoming or outgoing Internet connections on the company's network.
- 13.17 Users shall not use modem / wireless datacard / any other media to access internet while being connected to the LAN.

- 13.18 Use of personal Instant messenger and chat is prohibited. Very selectively when instant communication is necessary over the internet to perform certain activities because of business demands, Instant messenger shall be made available.
- 13.19 Violations of the Internet usage Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.
- 13.20 All e-mail IDs maintained on the individual system is specific to the system and is to be taken care of by each individual user.

## **14.0 Backup / Restore Procedure**

### **14.1 Backup Procedure**

#### **14.1.1 Server Backup**

##### **i) Database Backup**

- a) Daily full backup of database is taken on the Storage disk and same is backed up on the tape drive.
- b) Tape drive has 8 slot tape drive scheduled for 7 days and one drive used for cleaning tape to clean the drive.
- c) At any given time IT has 7 days backup on the tape drive and every month IT closes 2 tapes i.e. on 1<sup>st</sup> & 10<sup>th</sup> of every month which means that IT removes 2 tapes and it is stored in special fire proof & temperature controlled cupboard. HO backup tapes will be kept at Rabale and vice-versa for safety.
- d) The backed up tapes will be kept in custody for a period of 6 months after which the same will be formatted and reused for backup. This process will be carried out for 3 backup cycle of the tape.

##### **ii) File Server Backup**

- a) Daily full backup taken on the tape drive.
- b) Tape drive has 8 slot tape drive scheduled for 7 days and one drive used for cleaning tape to clean the drive.
- c) At any given time IT has 7 days backup on the tape drive and every month IT closes 1 tape i.e. on 1<sup>st</sup> of every month which means that IT removes 1 tape and it is stored in special fire proof & temperature controlled cupboard. HO backup tapes will be kept at Rabale and vice-versa for safety.

- d) The backed up tapes will be kept in custody for a period of 6 months after which the same will be formatted and reused for backup. This process will be carried out for 3 backup cycle of the tape.

### iii) Instrument System Data Backup

- a) Daily backup of Instrument data is automatically scheduled or manually taken on the computer attached to the instrument.
- b) The incremental backup is backed up on a separate server/storage connected on that network on a daily basis.
- c) Daily incremental backup of storage is taken on the tape drive.
- d) Tape drive has 8 slot tape drive scheduled for 7 days and one drive used for cleaning tape to clean the drive.
- e) At any given time IT has 7 days backup on the tape drive and every month IT closes 1 tape i.e. on 1<sup>st</sup> of every month which means that IT removes 1 tape and it is stored in special fire proof & temperature controlled cupboard. HO backup tapes will be kept at Rabale and vice-versa for safety.
- f) The backed up tapes will be kept in custody for a period of 6 months after which the same will be formatted and reused for backup. This process will be carried out for 3 backup cycle of the tape.

### iv) User Data Backup at Plant - Waluj

- a) Weekly once backup of user data is automatically scheduled on the server.
- b) Daily backup of server/storage is taken on the tape drive.
- c) Tape drive has 8 slot tape drive scheduled for 7 days and one drive used for cleaning tape to clean the drive.
- d) At any given time IT has 7 days backup on the tape drive and every month IT closes 1 tape i.e. on 1<sup>st</sup> of every month which means that IT removes 1 tape and it is stored in special fire proof & temperature controlled cupboard. HO backup tapes will be kept at Rabale and vice-versa for safety.
- e) The backed up tapes will be kept in custody for a period of 6 months after which the same will be formatted and reused for backup. This process will be carried out for 3 backup cycle of the tape.

**v) Data Backup at Plant – Baddi - I**

- a) All HPLC Data is being stored on Chromeleon Server.
- b) All Other Instruments data is being stored on Local Instrument E: Drive. Then copied to Virtual Server twice a day. This data is copied to Chromeleon server for backup on tape.
- c) Scada / Track and Trace And Oasis application data are manually copied to Chromeleon server for backup on tape.
- d) Daily fully backup. Two separate tape for each day. Tape is replaced on daily basis.
- e) Monthly secondary backup on separate tape for each month.

**vi) Data Backup at Plant – Baddi - III**

- a) All HPLC Data is being stored on Oracle Empower Server.
- b) All Other Instruments data is being stored on Local Instrument E: Drive. Then copied to Empower Server with Script.
- c) Empower Server (Oracle – Hot/Cold backup) and Other Instrument backup copied to Chromeleon Server for backup on tape.
- d) Daily fully backup. Two separate tape for each day. Tape is replaced on daily basis.  
Monthly secondary backup on separate tape for each month.

**Note -**

- i) **Current Process at Baddi** – User data backup is taken on USB hard disk and instrument data is backed up on the computer attached along with the system and subsequently the backup is taken on a separate computer attached on the network. This data is copied onto a CD /DVD, a copy of which has to be sent to HO every month.

**14.1.2 Email Backup**

- i) It is the responsibility of the individual user to take backup of their E-mail on their computer drive. The user can take guidance and help from the I.T. personnel available for doing the same.
- ii) It is the responsibility of individual user to archive their old mails every 3 months. In case of large no of mails, there are chances of the mailbox getting corrupt and loss of mail. The user can contact IT for guidance in archiving / backup.

#### **14.1.3 Laptop / Desktop Backup**

- i) It is the responsibility of each user to maintain or backup all official files on the Network drive provided. Users designated Associate Vice-President and above, will be provided with a separate USB Hard disk for taking backup of their Laptop / Desktop data including E-mail. This Hard disk will be in the custody of the respective user. In case of any help required in taking backup, the respective user should intimate the IT department for the same.

#### **14.1.4 Website Backup Policy for Indoco Websites**

- i) IT Department to provide access of Network Drive to the In-house Web Designer to create website-backup folder and take backup in the respective folder, for example "Y:\Website-Backup". IT department to provide sufficient space and access rights for the web designer to carry out backup task.
- ii) All the Indoco owned Websites should be backed-up in this folder into Sub-folders with individual website names. The Web designer should take the backup at least once every month. If any changes / additions are done to the individual websites, the same should be uploaded to the backup folder on the same day by the In-house Web designer. Storage capacity should be increased as and when required.
- iii) The Publically Accessible "Archive" section will also be backed-up on the Network Drive "Website-Backup" folder by the In-house Web designer.
- iv) The In-House Web Designer's PC should be provided with a high speed internet connection for the purpose of backup and restore activity of all websites. Regular retrieval and checks should be carried out by the In-house Web designer to verify the contents of Indoco websites backed up on the Network drive.
- v) Networking team from IT Department will be responsible to maintain the latest backup of the "Website-Backup" folder from the Network Drive on to a Tape Drive or any other reliable backup system.

14.1.5 IT department will maintain records of the server backups taken. A separate register will be maintained keeping track of date of backup and bar code of tape drive if available. This will be signed by the concerned IT personnel and checked by his superior.



## **14.2 Restore Procedure**

- 14.2.1 In case of any need to restore backup due to corruption / failure in data access, the last backed up data will be restored only after being confirmed by the concerned user and approved by the department head / section head / operations head / management.
- 14.2.2 IT department will make random checks of backups taken by restoring them on a separate test server and will document the process.

## **14.3 Re-usable of Backup Media**

- 14.3.1 The backed up tapes will be kept in custody for a period of 6 months after which the same will be formatted and reused for backup. This process will be carried out for 3 backup cycle of the tape.

## **15.0 I.T Procurement – Systems (Desktop / Laptop / Printer / Scanner)**

### **15.1 I.T Procurement Process**

#### **15.1.1 Locations / Plants / Sites**

- a) Indenters mail to respective HOD for approval.
- b) Approved HOD mail to Plant Head / Location Head / Site Head
- c) Plant Head / Location Head / Site Head approved mail to Local I.T Head.
- d) Local I.T. head will understand the requirement and accordingly action will be taken.

Action as follows:

- i) Stock in hand transfer
  - 1) Local IT will transfer existing stock at their location or will send a request to HO IT for availability at other locations.
  - 2) HO IT will analyze the requirement for transfer of stock from other locations based on availability and need.
  - 3) HO IT dept. will send a detailed list of hardware transferred from other locations to Accounts dept. for making necessary entries in the financial books.
- ii) Upgrade if possible

- 1) Local IT will analyze the requirement and send mail to HO IT with justification.
  - 2) HO IT will analyze the requirement and will take action as defined in point 15.1 – 15.1.1 – iii - 6
- iii) New requirement
- 1) Local IT will raise the indent in the standard material requisition format of the company based on the Eligibility criteria and configuration policy given below along with Budget code if available.
  - 2) Approved mail from Plant head including the trail mails to be attached.
  - 3) Minimum two quotations to be attached.
  - 4) Above referred documents to be sent to Operation Head for approval.
  - 5) Operation head approved indent will be sent to HO I.T.
  - 6) HO I.T. will analyze the requirement and will take action.
    - In case of rejection, the document will be sent back to Local I.T with proper reasoning
    - HO I.T. will mark the requirement as Budgeted (with Budget code) or Non Budgeted with justification for the same.
    - If approved, Indent will be sent to Purchase for taking further approvals as per the stages mentioned below
      - Approval from Head I.T
      - Approval from Head - Purchase
      - Approval from President – Finance
      - Approval from Management (Managing Director /Joint Managing Director)
- iv) Rejection – In case of rejection by Local IT, the document will be sent back to Indenter with proper reasoning.
- e) Final Approved Indent will be sent to Purchase for further negotiation and procurement.

#### 15.1.2 At Head Office

- a) Indenters mail to respective HOD for approval.
- b) Approved HOD mail to HO IT.
- c) HO I.T. will understand the requirement and accordingly action will be taken.

Action as follows:

- i) Stock in hand transfer
  - 1) HO IT will analyze the requirement and will either proceed with transferring

existing stock in hand or opt for transfer of stock from other locations based on availability and need.

2) HO IT dept. will send a detailed list of hardware transferred from other locations to Accounts dept. for making necessary entries in the financial books.

ii) Upgrade if possible

1) HO IT will analyze the requirement and will take action as defined in point 15.1 – 15.1.2 – iii – 5

iii) New requirement

1) HO IT will raise the indent in the format attached in standard material requisition format of the company based on the Eligibility criteria and configuration policy given below.

2) Approved mail from respective HOD including the trail mails to be attached.

3) Minimum two quotations to be attached.

4) HO I.T. will mark the requirement as Budgeted (with Budget code) or Non Budgeted with justification for the same.

5) HO I.T will send indent to Purchase for taking further approvals as per the stages mentioned below

➤ Approval from Head I.T

➤ Approval from Head - Purchase

➤ Approval from President – Finance

➤ Approval from Management (Managing Director /Joint Managing Director)

iv) Rejection – In case of rejection, the document will be sent back to Indenter with proper reasoning.

d) Final Approved Indent will be sent to Purchase for further negotiation and procurement.

## 15.2 Configuration of Systems

### a) Desktop

- i) All systems procured will be branded.
- ii) Standard configuration as given below should be procured unless otherwise specified in point iii below. The standard configuration will be reviewed from time to time by HO IT and necessary changes will be carried out with the approval of Managing Director / Joint Managing Director  
Processor – I3 Gen 6  
RAM – Min 4 GB  
HDD – Min 500 GB or Minimum available HDD  
Monitor – 18.5" LED
- iii) Desktops which are to be connected to Plant systems like HPLC, GC etc or to any Third party software and requirements as per third party vendors etc, the configuration will be as per the Vendor specifications which will be analyzed by IT department in consultation with respective department head and Vendor before being finalized by HO IT.

### b) Laptop

- i) All systems procured will be branded.
- ii) Standard configuration as given below should be procured. The standard configuration will be reviewed from time to time by HO IT and necessary changes will be carried out with the approval of Managing Director / Joint Managing Director.  
Processor – I3 Gen 6  
RAM – Min 4 GB  
HDD – Min 500 GB or Minimum available HDD  
Monitor – 15.5" LED.
- iii) Procurement will be based on the Laptop Eligibility Criteria given below in point 15.3.

### c) Server

- i) Servers will be procured based on Vendor specification which will be analyzed by IT department in consultation with respective department head and Vendor before being finalized by HO IT.

**d) Printers / Scanners / Switches etc..**

- i) Configuration will be analyzed by IT department in consultation with respective department head and Vendors (if any), before being finalized by HO IT.

**15.3 Laptop Eligibility Criteria**

- i) Laptop will be provided to employees whose jobs include regular travelling, dept like PMT, Sales, International Business, Internal Audit, Credit Control and Information Technology where support is required after office hours.
- ii) Laptop will also be provided to all employees designated Assistant General Manager and above designations.
- iii) Laptop will be procured as per the below given conditions :

Designation	Limits without including Cost of Operating System (OS)
Below Assistant General Manager	Rs. 30,000/- To Rs. 40,000/-
Above Assistant General Manager & Below President	Rs. 45,000/- To Rs.55,000/-
President & Above	Rs. 60,000/- To Rs. 80,000/-

- iv) The Laptop eligibility criteria will be reviewed from time to time by IT and necessary changes will be carried out with the approval of Managing Director / Joint Managing Director

**16.0 I.T Procurement – Internet / MPLS – VPN / Storage**

**16.1 I.T Procurement - Wide Area Network / Internet / Wireless / Routers/Storage etc.**

- i) MPLS VPN / Internet / Wireless / Routers / Storage etc will be procured based on the analysis of requirements by IT department.
- ii) Process to be followed :
  - 1) HO IT will raise the indent based on the requirement analyzed by IT.
  - 2) Quotations from service provider to be attached.
  - 3) HO I.T will take further approvals as per the stages mentioned below
- v) Approval from Head I.T
- vi) Approval from President – Finance

- vii) Approval from Management (Managing Director /Joint Managing Director)
- iii) Final Approved Indent will be sent to Purchase for further negotiation and procurement.

## **17.0 Replacement of System**

### **17.1 Desktops**

- i) Desktops will be replaced after a period of 5 years from the date of installation.
- ii) Procurement will be done as per the eligibility criteria and configuration policy as applicable at the time of replacement.

### **17.2 Laptops**

- i) Laptops will be replaced after a period of 4 years from the date of installation.
- ii) Procurement will be done as per the eligibility criteria and configuration policy as applicable at the time of replacement.

### **17.3 Servers**

- i) Servers will be replaced after a period of 5 years from the date of installation.
- ii) Procurement will be done as per the requirement analyzed and finalized by HO IT.

### **17.4 Storage / Switches / Routers**

- i) Storage will be replaced after end of life defined by the OEM or support withdrawal by OEM.
- ii) Procurement will be done as per the requirement analyzed and finalized by HO IT.

## **18.0 I.T. System – Damages and Recovery**

- 18.1 In case of physical damage to Laptop, if it is due to wear and tear of the Laptop the cost of repair would be borne by Company. In all other instances the repair cost for the same would be recovered from the User to whom the Laptop is allotted.

- 18.2 In case of physical damage to Laptop where the Laptop is not repairable or in case of theft/loss of Laptop the cost would be recovered from the User to whom the Laptop is allotted. This amount would be Minimum Rs. 10,000/- or the cost of Laptop in the books of accounts as on the date whichever is higher.
- 18.3 In case of physical damage to Desktops and other I.T. system, the cost for repair / replace would be borne by Company.

### **19.0 Disposal of I.T. System**

- 19.1 A list of obsolete hardware for disposal shall be prepared by the I.T personnel at locations and forward it to HO IT thru Plant head. This activity will be performed on half yearly basis.
- 19.2 The I.T. personnel shall prepare the list with reasons for its obsolescence and for recommendation for disposal
- 19.3 HO I.T. shall vet the list and suggest further measures such as sale to employee or sale as scrap and forward it to Head – Accounts for further recommendation and approvals.
- 19.4 On receipt of approval for disposal from Accounts, IT at HO or Location as the case may be, shall forward the approved list to Administration dept. Administrative dept. shall carry out all formalities for sale to employees or sale as scrap.
- 19.5 On receipt of the approved list, Administration dept. shall invite competitive rates from at least 3 vendors.
- 19.6 In case hardware is proposed to be sold to employees, then the rates quoted by the highest vendor should be the sale price to the employee. A circular informing the same should be sent to employees. Allotment to employees will be on "First Come First Serve" basis and should be sold on "As-It-Is" basis. This offer should be time bound and closed within 1 week of the circular. The hardware not opted by employees should be sold to the vendor quoting the highest rates.
- 19.7 The proceeds from disposal shall be deposited with the cashier or the cheque to be forwarded to Accounts dept. as the case may be.
- 19.8 Administration dept. will send a detailed list of hardware disposed to Accounts dept. for making necessary entries in the financial books and raising invoices as required.

## 20.0 Archival of Website Information

- 20.1 Any information / document / data shared on the company's website will be displayed for a period of 5 years from the month of uploading the same onto the website.
- 20.2 The Legal Department should specify the pages and information which needs to be maintained on the Website as a Publically Accessible "Archive", such pages / information should be older than 5 years from the month of uploading the same on the website.
- 20.3 The Legal department should specify when the pages and information maintained on the publically accessible "Archive" will be removed from the Archived section.


## 21.0 POLICY REVIEW

- 21.1 The Policy shall be subject to review as may be deemed necessary and in accordance with any regulatory amendments and Managing Director / Joint Managing Director will approve any amendments.

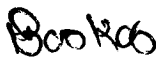
Prepared by:

\_\_\_\_\_  
(Prakash Shukla, Executive Senior Manager - Information Technology)

Reviewed by:

  
\_\_\_\_\_  
(Biju Nair, General Manager – Information Technology)

Approved by:

  
\_\_\_\_\_  
(Mandar Borkar, Vice President and CFO)

Approved by:

  
\_\_\_\_\_  
(Managing Director / Joint Managing Director)