Sharda Motor Industries Limited

Version	:	1.0.0
Reviewed by	:	Head – IT / ERP
Approved by	:	CFO
Effective date	:	01/08/2018
Total No. of pages	:	32
Distribution details	:	Hard Copy / MAIL

IT MISSION

If the solution that enriches business exists,

We must find it.

If it does not, we must create it.

IT VISION

Enhance and Sustain an Environment of

Trust, Accuracy, Reliability

By maximizing Integration and Automation

For Meeting Business Objectives

With Complete Customer Satisfaction

At the lowest possible cost and with latest Technology.

Introduction

All employees share the Information Technology facilities. These facilities are provided to employees for the purpose of conducting Company's business. The Company does permit a limited amount of personal use of these facilities, including computers, printers, e-mail and Internet access. However, everyone must use these facilities responsibly, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt company business and interfere with the work or rights of others.

It is the responsibility of all operating units to ensure that these policies are uniformly followed, both in letter and Spirit.

Coverage

These policies cover the usage of all of the Company's Information Technology resources, including:

All computer-related equipment, including desktop personal computers, databases, printers, servers, CD writers, Scanners, all networks and hardware to which these equipment's are attached.

All electronic communications, including e-mail, Internet and Intranet.

All software including purchased or licensed business software applications, Company-written applications, computer operating systems and any other software residing on Company-owned equipment.

All intellectual property and other data stored on Company equipment.

Owner

Head IT Department.

HARDWARE POLICY

Intent

The intent of this policy is to establish standard practices and guidelines for the Procurement & proper maintenance of company's IT Infrastructure and makes the users aware of what SMIL Group deems as acceptable and unacceptable use of its Infrastructure.

Scope

This policy is applicable to all the members of SMIL Group.

Hardware Coverage, Procurement, allocation

All Information technology Equipment's

1. Requirement of Desktop / Laptop, HR Dept will give the request of Desktop / Laptop to IT for the new user. HR will get the confirmation of availability of Desktop / Laptop with IT If available, then the same will be provided to the new user else IT will have to raise CAPEX Indent as per Format No. as **Annexure-2** and get it signed by the appraising authority as per policy.

2. All Desktops/Laptops will be procured with software licenses of Operating System and other related software as per need of user job profile.

3. Laptops will be procured only for need base (purpose should be specified) or special recommendation from departmental head and final approval from COO as per Format No. SMIL/IT/Format -1.

4. Since laptop is expensive equipment and its Maintenance is costly, it is important that necessary guidelines be laid down for its procurement / purchase and subsequent usage / disposal.

5. SMIL will not be provide Desktop / Laptop to Trainees, exclusively under approval by COO.

Life of Desktop / Laptop / Printer etc.:

Generally, life of a Desktop PC / Laptop / Printer etc. would be as under:

a) The life of Desktop PC & Laptop etc. is for 5 years from the date of purchase and Printer for 3 years from date of purchase.
b) After 5 years of each Desktop PC/ Laptop and 3 years of Printer, IT will review the performance of the same.
c) If the equipment's performance meets the requirement at that time, then the same can be provided to the users.
d) If equipment does not perform according to requirement of users or equipment is outdated and parts of the same are not available, then the same can be disposed off after having approval from the Head -IT / CFO.

PROCEDURE FOR PROCUREMENT:

- A request for a new Laptop along with OS and Microsoft office for an employee will be raised by his HOD on the requisition format (Part 1) see Annexure 1
- This request duly vetted, justified and recommended by the respective HOD & approved by the COO will be sent to IT department for Asset Procurement.
- HOD- IT will endorse the necessary specifications; suggest the model and approximate cost of the laptop.
- If an old functional workstation (laptop/Desktop) meeting the required specifications is available in the IT Department, then HOD- IT may recommend the issue of the same.
- The Capex duly approved by COO for necessary purchase action will be forwarded to HOD-Purchase by the concern department HOD.
- Once the laptop is purchased, it will be delivered to the individual and a receipt will be obtained from the person as shown in the Annexure-I (Part 2).
- The employee can requisite for replacement of a laptop after five years through his/ her HOD as the case may be, by the same procedure as above.
- Should there be a necessity to replace a laptop before Five year due to technical reasons, the same be justified by the HOD which will be approved by Head -IT
- For Laptop capex has to be signed by HOD , Head -IT, Approved by CEO.
- Agreement between the user & the company will be made (refer Annexure II) for HR.
- Purchase department is completely responsible for managing all dealings with Vendors and Service Providers till purchase is done.
- Laptop has to be purchased as per recommended configuration by IT Department.
- IT Department will be responsible for Warranty, AMC & Extended warranties etc.
- System configuration mentioned in Annexure

Up gradation or Replacement

The Hardware replacement or up gradation will be given after 5 years or when the internal technology is upgraded, depending up on the latest technology available in the market and the users requirement.

In case the Laptop is not in the working condition same will be replaced after 5 years.

Laptop Bag

a) As and when any Laptop is purchased, an order for standard bag as per the OEM of laptop to be placed with the vendor. The cost of Laptop Bag should not be more than maximum Rs.1000/-. Any user requiring for a specific laptop bag, with cost more than Rs.1000/-, s/he will have to get the approval from COO.

b) Users are not authorized to purchase Laptop Bag independently without any consent of concerned IT.

THEFT /LOSS OF LAPTOP

In the event of theft, the user employee will be required to lodge an FIR with the nearest police station where the theft happened and approach the HR/IT Department, with a copy of FIR for further necessary action. The Laptop users will have direct responsibility and custody of their assigned Laptop. They may be held financially liable for any loss and / or damage to the Laptop due to inappropriate usage / carelessness.

GENERAL GUIDELINES

IT department will ensure that all the Laptop are covered under Annual Maintenance Contract or extended warranty after expiry of the warranty period. Company will obtain insurance coverage for Laptop to cover the eventualities such as theft, sabotage or damage which will be the responsibility of Issuance in charge.

IT Dept. will ensure that Laptop is protected for which IT may recall the Laptop for updating and return as per schedule.

TERMINATION OF EMPLOYMENT

1. On leaving the service of the Company, HR Department has to ensure that the employee hands over company's Laptop with all its accessories to the IT Department.
2. After receiving the Laptop & other Accessories, IT Department (Head-IT) will sign the NOC for further HR activities.
3. In the event of an employee absconding or any other unauthorized absenteeism, without handed over the asset, same will be deemed as offence and the Company will initiate legal action against such employee as per law of lands.

Use of Personal Laptop

The use of personnel laptop in company is strictly prohibited. The IT person will not configure the personnel computer for its usage in company. If anyone found using personnel computer in Group, it will have treated as misconduct and suitable action will be taken accordingly.

If it has to be used, Permission is required from appropriate authority i.e. Head of IT & HR Head.

IT person reserve the rights to deny or withdraw, the right to connect the personnel desktops, laptops, or any other IT devices onto Group network if the system does not comply with the IT Policy and report to appropriate authority.

All External storage devices like pen drives, external hard drives and other hardware equipment should be declared by the visitor to the gate security while visiting Group office/ Operation Location/ Campus. The security office should ensure the recording of these details, while issuing gate passes / that shall be displayed at all security gates.

Company's Responsibilities

The company is responsible for providing standard quality of IT infrastructure with proper preventive and corrective maintenance time-to-time.

All Computers will have the below mentioned standard suite of software installed, which will be supported by the IT Department.

Individual employee's requirement in relation to the software other than the above-mentioned list would be considered on case-to-case basis.

Hardware Sanction

The requirement owner needs to take sanction with justification in the specified format from the Concern HOD and which will finally be approved by IT Head/CFO/COO. Then it will follow the Hardware Purchase process as specified in this policy.

Hardware Allocation

Desktops & Laptops

Employees will be provided with computer access in the office either on one: one basis or on sharing basis as per their job requirement. The computer provided will be a desktop model as per the Technical specification, specified in the Hardware Policy with the standard software suit installed in it. Laptops will only provide when there is sufficient job-related rationale. When a laptop is allocated for individual use, it is allocated only in exchange of the desktop, not in addition to the desktop. Shared laptops will be provided to entire Plant based on sufficient rationale.

Senior employees required to move frequently and requiring information and data easily available with them all the time. Laptop provide important functionality, allowing employees to have their computing resource at hand in meetings/workplace, and those who travel on business to be maximally functional and productive while away.
The configuration of Laptop will be finalized by Head – Group IT.

Above category of employees can purchase any Laptop as per following limit.
Category A (L1-L2) : Elite Book I5,8GB, 512 SSD, 13.3" Approx. Rs.1.32L
Category B (L3-L5) : Think Book I5,8GB, 512 SSD, 14" / 15" Approx. Rs.88K
Engineering Workstation : Zbook I5/I7, 16GB RAM, 512 SSD, 15" Approx Rs.1.32L
R&D Work station :As per Software requirement (Cost will be varied)
MS Office cost is Separate: Rs. 0.16 Lacs for all
Brand - HP / Dell / Lenovo (Depend on Availability / Cost

Depending upon the nature of the job, COO /CEO may approve laptop for other level of employees also, however, cost of such laptop should not exceed Rs. 88,000/-.

On issuing the Laptop to employee, unit HR to obtain company asset take over form and the same will be filed in the personal file of the user.

As technology is changing fast, laptops are also required to be updated regularly. Laptop can be replaced once in Five /Four/Three years depending on the recommendation of IT department. In such case old laptop can be sold to the supplier in buy back scheme.

Printers

Employees are not automatically provided a personal printer as part of the standard office computer allocation. Individual printers are provided upon request. The printer allocated for individual use is based on the rationale provided. Generally, color inkjet printers will be allocated. In some instances, it may be appropriate to allocate a shared laser printer. Shared laser printers will generally be placed one per floor. One member from the departments who share the printer will be responsible for maintaining, refilling the cartridges.

Moving Computer Equipment or IT asset

Shifting of Desktop PC

Desktop PC cannot be shifted from one place to another place without written permission as per Format No. SMIL/IT/Format-2 from Admin Dept. in consultation with IT.

Data Transfer from one PC / Laptop to another

User Data can be transferred from one user to another user PC / Laptop with the written permission of HOD as per Format No. SMIL/IT/F0003.

Transfer of IT Assets

Assets purchased in the name of a unit will remain there. Nobody is allowed / permitted to carry IT Assets with him to another unit, if he has been transferred – i.e. Laptop etc. The Laptop issued to an employee by a unit / branch office, has to be surrendered by him while s/he is being transferred. S/He has to get a laptop from the unit, to which he has been transferred.

Alternatively, any Asset can be transferred to another branch office/unit of the same unit after getting proper clearance from Accounts Dept. of a Unit.

HARDWARE & NETWORK USAGE POLICY

Intent

The intent of this policy is to establish standard practices and guidelines for the safe, productive, optimal & proper use of company's IT Infrastructure and makes the users aware of what SMIL Group deems as acceptable and unacceptable use of its Infrastructure.

Scope

This policy is applicable to all the members of SMIL Group.

Hardware Usage

The productive and effective use of Company's Hardware can only be achieved if we have proper utilization of all hardware resources and Software licenses, as they are very expensive and vital for the Company.

The policy prescribes proper sharing of all available Hardware resources allotted to the individual departments. All HOD's are required to ensure the same.

The functions and level of sharing is mentioned below:

Domain, System, Mail User Id Policy Nomenclature Domain/System/mail id for Users

This policy is designed to standardize domain user name, system name and email id of users.
The following policy for Domain, Systems & mail ID are in force and to be followed by individual Units.

- Domain User ID should be user Name
- Mail ID should be user name
- Local user password of system should be common for all users and user can change password next logon.
- Administrator Password should be changed Monthly and / or change as and when required.
- No user has the rights to install any software / download.

Network Documentation Policy

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy help us to reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

Cyber Security Policy - Network/Gateway

This policy is designed to protect the organizational Network and resources against intrusion by viruses, malware spyware and unauthorized access of network.

Organization is using Firewalls for protection from hackers, anti-virus, anti-spam, AV definition, intrusion prevention, IPS definition and web filtering. The following policies for Network/Gateway security have been in force.

1. Firewall of different configuration are working to cater all locations
2. Firewalls are configured for real time policy enablement.
3. Firewall library definitions updated automatically at regular intervals.
4. Only administrator has the privilege to change firewall configuration in regard of all services.
5. No Down load is permitted thru website.
6. No users are allowed to chat through Google Talk, Face Book, Yahoo Messenger, U-Tube, MSN Messenger etc. for the data security.
7. IP Scheme for network:

The network scheme for local area network connect thru following series have been applied.

Security Policy – Servers

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords and establishing a minimum time between changes to passwords.

1. Minimum Length - 8 characters
2. Maximum Length - 14 characters
3. Minimum complexity - Passwords should use following three types of characters:
   I. Alphabet
   II. Numbers
   III. Special characters such as! @ # $ % ^ & * ( ) { }[ ]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 3.
6. Maximum password age - 30 days
7. Minimum password age - 15 days
8. Reset account lockout after - 5 Minutes.
9. Account lockout duration - 5 Minutes

Server Monitoring Policy

This policy is designed both to protect the organization against loss of service by providing minimum requirements for monitoring servers. It provides for monitoring servers for file space and performance issues to prevent system failure or loss of service.

Organization is using multiple servers to cater different type of services required to run from basic infrastructure to special applications. We have following policies for server monitoring in force.
The following servers are being checked manually on daily basis.

User Responsibilities

Company wishes users to adhere to the following guidelines

Maintenance

- Download Latest Patches for virus every week from the central server.
- Keep the computer and devices neat and clean.
- Run Scandisk on weekly basis.
- Run De-Fragmentation Utility on Monthly basis.
- Run Virus Scan on Daily basis.
- Ensure that its Preventive is carried out timely i.e. after every 3 Months.
- Ensure CPU must have Uninterrupted Power Supply.

Acts Strictly Prohibited

- No Software or updates can be installed without taking written approval from IT Department.
- Floppies, CD's, Pen drives should not be used, without scanning them for Viruses.
- No Unlicensed Software should be installed in the system.
- No other copies of any software or its documentation should be made.
- Improper Shutdown should not be done.
- Standard Windows background or Corporate Background must be used.
- Screen Saver should not be used.
- Booting password in BIOS should not be given.

- Dial up connections should not be used wherever the firewalls are installed.

INTERNET POLICY

Intent

The intent of this policy to establish standard practices and guidelines for the responsible, safe, and productive use of the Internet, and to ensure the protection of SMIL Group's information infrastructure. The Policy is to ensure that access to the Internet, as authorized by SMIL Group is used primarily for the conducting of Company business, and is not used for illegal, offensive or unethical use. The policy also prohibits such access for conducting non-Company commercial business, and for excessive and non-productive personal use, such as playing games, or excessive personal investment activity.

Scope

This policy applies to all employees when they are using Internet connections supplied by SMIL Group.

Company's Responsibility

The company is responsible for providing Internet round the clock to approved users and ensures 99% up time, where we have dedicated Internet Band width. In case of Dial up connection, Internet will be available on need basis.

Users Responsibility

Equipment and information in any form is considered an asset of the Company and thus must be properly used and adequately protected. This includes the usage of company provided Internet, which are to be used primarily for business purposes.

Company wishes users to strictly adhere to the following guidelines.

Overall Internet Usage Do's & Don'ts.

1. Internet connectivity will be available to everyone, one those authorized by the management will have the access to some defined sites.
2. Use of public IMs such as Yahoo and MSN is strictly prohibited in the company.
3. Don't download unnecessary software, songs or videos. These take up significant Internet bandwidth.
4. Use of public website, Naukri, job street and other non-official site will not be allowed.
5. Installing software other than official and download accelerators is not allowed.
6. Don't visit objectionable Web sites containing bad language and pornography, Web site access is monitored centrally and anyone found to be doing so would be sent a warning.
7. Visiting casual Web sites is not permitted during office hours.

Acts Strictly Prohibited

- Jokes, Cartoons, Pictures, Screen savers, Music files, etc should not be downloaded.
- You should not download or use material from the Internet in violation of software licenses, or the copyright trademark and patent laws.
- Dial up connections should not be used wherever the firewalls are installed and dedicated Internet access is available.
- User shall not install or use any software obtained over the Internet without written permission from the Corporate IT Department.

Users Classification

Internet users are classified into three categories. The categories are

S. No.	Category	Designations	Precincts
1.	Top Management	Chairman, CEO,COO, CFO, President	• All the above sites will be open except some restricted Sites. • Social Networking is open. • Download & Upload is open. • Webmail is open.
2.	Management	VP/ AVP GMs, AGMs/	• Some of the above sites will be open except Phonography. • Web browsing (news & General information etc.) will be open. • Webmail is open. • Social Networking is open.
4.	Sr. Staff / Staff	Sr. Managers, Manager, Dy Manager, Asst Manager, Sr. Exe & Executive.	▪ All the above will be Blocked. ▪ Web browsing (news & General information etc.) will be open. ▪ Webmail will be blocked. ▪ Social Networking is blocked.

Internet Access

Internet Access will be available for all employee as per policy.

EMAIL POLICY

Intent

The intent of this policy is to establish standard practices & guidelines for the responsible, safe, productive and proper use of company's electronic mail (email), to ensure the protection of our information infrastructure and make users aware of what SMIL Group deems as acceptable and unacceptable use of its email system.

Scope

This policy is applicable to all email account holders of SMIL.com.

Email Account

All email accounts maintained on our email systems are property of SMIL Group. Therefore, all messages distributed via the Company's email system, even personal emails, is SMIL Group's property. The user has no explanation of privacy in anything he / she creates, stores, sends or receives on the Company's email system. The emails can be monitored without prior notification if SMIL Group deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action.

Email account will be offered to all employees of SMIL Group & associates and accounts not used for 180 days will be deactivated / possibly deleted.

Email Addresses

SMIL Group will provide email address in a standard format

Only one destination address is allowed to be maintained by one person at one time.

EMAIL SIGNATURE in (Arial 11 & 10pt)

Thanks & Regards,
Name of Person
Designation

Sharda Motor Industries Ltd. | D-188, Okhla Phase-1 | New Delhi-110020
Phone- +91(11) 47334100 Ext. No-…….
Email ID: xxxx.xxxxxx@shardamotor.com | Web: www.shardamotor.com

Guidelines for E-mail signature:

Thanks & Regards - Arial – 10 Bold.
Name - Arial - 11,
Designation - Arial -11
Company Logo
Company name - Arial 11 Bold
Company Address, telephone, mobile phone, e-mail etc. - Arial -9
Disclaimer Heading - Arial – 7 Bold
Disclaimer Text - Arial – 6

Company's Responsibility

The company is responsible for creating and managing an infrastructure that can support the safe and successful delivery of email within the company, partners and others via the Internet round the clock.

As part of this architecture, the Company will create means by which it can scan the content of message to prevent the spread of viruses, worms, Trojan Horses, or other executable items that could pose a threat to the security of the system and network.

Email that has been found to be infected with virus, worm, Trojan horse, or contains another executable item could pose a threat to security will not be delivered to the user. Infected email will be first cleaned and if not cleaned will then be removed from the delivery system and analyzed by network and security administrator.

Access to email account will be available 24 X 7 days with an up time of 98%.

Email Space Allocation

All emails account will be given space of 2000 MB, if more space is required then written approval of from IT-Head/CFO is to be taken.

User Responsibility

SMIL Group considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer support. Users should take the same care in drafting an email as they would for any other communication. Therefore, Company wishes users to adhere to the following guidelines.

Overall E-mail Usage Do's & Don'ts.

1. While everyone likes to read a good joke once in a while, please don't make it a habit. Avoid sending jokes to huge mailing lists.
2. If you get a mail that's been forwarded to a long list, don't hit the Reply All button if you only need to inform the sender.
3. Avoid sending huge attachments in e-mail, unless it's official. Also, even if it's official, avoid sending it to a colleague in the same office, save the attachment on the file server and send a plain mail intimating the recipient to pick it up from common Folder.

4. Avoid subscribing to any news sites on the Web with your official mail id. These are a major cause of spam
5. Don't reply to any spam mail, even if it gives instructions to do so. This will actually confirm your presence to the spammer and you could be spammed even more.
6. Beware of opening e-mail attachments, unless you're sure that it's from a reliable source, and that you were expecting it. If necessary, call up the sender to check

Replying to emails

- Email should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hrs.
- Priority emails are emails from existing customers and business partners.

Maintenance

- Delete any email message that is not needed.
- The mailbox should be periodically cleaned so that, it does not exceed the allotted space.
- Passwords should not be given to other people and should be changed once a month.

Personal Use

Although the Company's email system should be used for business purpose, SMIL Group allows personal usage, if it is reasonable and does not interfere with the work. The company reserves the right to decide this.

Acts Strictly Prohibited

- Send or forward emails containing libelous, defamatory, offensive, racist or obscene remark.
- Send unsolicited email message. • Forge or attempt to forge emails message.
- Disguise or attempt to disguise your identify when sending mail.
- Send email message using another person's email account.
- Forward a message or attachment to another user, without prior permission of the originator.

IT TRAINING & DEVELOPMENT POLICY

Intent

The intent of this policy is to specify the base level of information technology (IT) skills expected in all incoming members of SMIL Group and to provide appropriate opportunities to all members, so that their skills are further developed as per their Job and Company's requirement.

Scope

This policy applies to all employees SMIL Group.

Company's Responsibility

SMIL Group will be responsible to provide an infrastructure, so that all members of the Group can be imparted training from time to time, depending upon their job requirement and future development.

IT training for all staff of SMIL Group will be made available to a standard at least equal to the base level required or specified by the Companies Training Department.

Members of IT are required to have proper training skills and Knowledge, so that they can further impart training and develop employees.

Users Responsibility

It will be the responsibility of all members of SMIL Group to acquire the basic information technology skills, working skills as required by them from time to time in co-ordination with the Company's Information technology Department.

Members of IT Department are required to enhance their skills in the Area of Information technology, so that they are up dated on the latest changes and development in the area of Technology.

All the Members of IT Department and the Support Team located at various units is required to attend the three days in – house workshop (OJT) which will be conducted by IT Department once in a year or IT staff will go to each unit and upgrade them.

SUPPORT POLICY

Intent

The intent of this policy is to establish standard practices and guidelines in order to provide prompt Hardware and Application related support to all the users in SMIL Group.

Scope

This policy is applicable to all the members of SMIL Group.

Hardware Support

Telephonic support for diagnosing hardware problems will be available 24 hours a day, 7 days a week, 365 days a year by the IT Support Team located at Corporate and by IT representatives located at various factory Locations.

All Hardware including Network will be under AMC, with a reputed company, who will be responsible for marinating Hardware, peripherals, and Network.

An average uptime of 97.5% will be accepted with the AMC provider. The AMC provider will provide onsite support within 120 minutes of the Call Logging time.

Any fault in parts will be attended as per the AMC Contract.

Application Support

Telephonic support for diagnosing application problems will be available 24 hours a day, 7 days a week, 365 days a year by the IT Support Team located at Corporate.

All calls shall be attended within 30 minutes of the Call Logging Time and will be resolved within 4 working hrs.

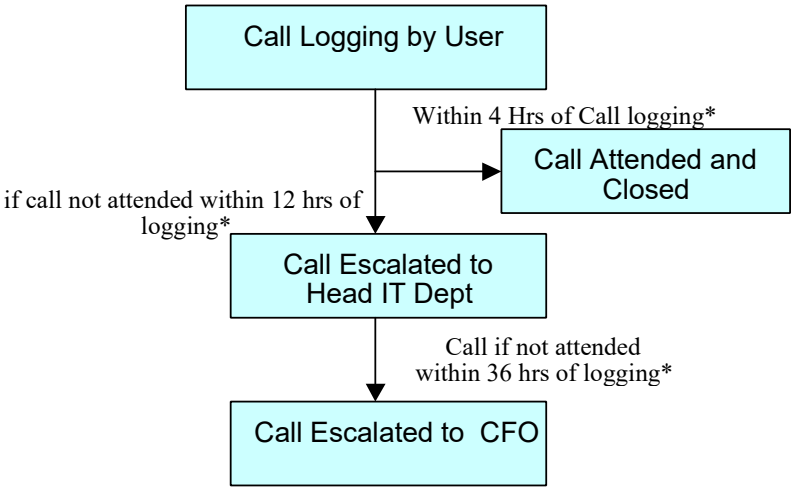
Department's Responsibility

All calls related to hardware and Application should have separate User call No, which should be provided to the user which logging the complaint. This no should be referred at the time of any further query.

Users Responsibility

All users are required to take User call No from the IT Department or by the IT Representative located in the Unit at the time of logging in the Complaint. All call shall be deemed valid only if they have the User Call No.

Call Escalation Process



* All hrs are calculated on the basis on Business Working Hrs.

Support Matrix

Head -IT

ERP	IT
1. Manager ERP (Techno Function)	1. Ass. Manager (Infra)
2. Manager ERP (Functional)	
3. Sr. Executive (Master Data Management)	

Users Survey

User satisfaction survey shall be conducted by the Corporate IT Department in each Quarter to find out their serviceability and promptness in resolving the user calls.

PASSWORD POLICY

Intent

The intent of this policy is to establish standard practices and guidelines in order to provide proper protection and security to various user documents and applications, by restricting access of every one in and outside SMIL Group.

Scope

This policy is applicable to all the members of SMIL Group.

SMIL Group uses Login ID and password as the method of authenticating users.

Administrators Responsibility

All system level passwords should be changed once in every quarter.
All production system level passwords must be a part of Administrative Global password management database.

Users Responsibility

All user level passwords should be changed once in every six months.

Does

- Passwords must be at least eight alphabetic character long.
- All Passwords must be declared to the Departmental / HOD so that the data can be retrieved in the absence of the User.
- A strong password must contain Upper and Lower case character.

Don't

- Preferably Password should not be a word found in a dictionary.
- Preferably passwords should a common usage word such as "1234", "company's name", "your own name".
- Do not reveal the password over the phone to anyone.
- Do not reveal a password in an email message.
- Do not share your password with other co-workers.

Data Backup Policy

I. Purpose and Scope

1. The purpose of this policy is as follows:
   - To safeguard the information assets of units of SMIL.
   - To prevent the loss of data in the case of an accidental deletion or corrupted of data, system failure, or disaster, whatsoever.
   - To permit timely restoration of information and business processes, should such events occur.
   - To manage and secure backup and restoration processes and the media employed in the process.

Data Card Policy

SCOPE

The policy contains the SMIL rules and procedures with regard to the Usage of Data Cards.

GENERAL

1. The data cards will be available for official use to the staff of SMIL and has to be utilized in a responsible manner.
2. Data Card facility will be given only when Staff is OUT OF OFFICE for official work.
3. If HOD or any other Senior Person is going on Leave and needs to be online with office will be given the Data Card.
4. Data Card is the Property of SMIL and any damage to it will be borne by the user.
5. As marketing is required to be online always so Marketing-Head & Second in line will be allowed Data Card on permanent basis maximum to 2 numbers and IT to connect with Online with Server Monitoring.

PROCEDURE TO AVAIL THE DATA CARD FACILITY

1. Spare Data Cards will be available with IT Department.
2. The Applications Form (as per Annexure-I) should be filled & approved by the concern HOD. This approval can also be taken by email.
3. All applications should be submitted to IT after approval before 24 hours of the requirement.
4. IT will arrange the instrument and issue the same to the user.
5. Once the requirement is completed, Users has to submit the Data Card back to IT.

Issuing of Data Card on Permanent Basis

1. All Data Cards will be issued & administered by IT.
2. If the Data Card requirement is Permanent, same has to be approved by the HOD / CEO.
1. A member of staff who is awarded a data card is personally responsible for the instrument and in case of loss amount as applicable will be deducted.

2. In the event of theft user have to lodge a FIR with the nearest police station immediately where the theft happened and approach the HR/IT Department with a copy of FIR for further necessary action.
3. A member of staff who is awarded a data card is personally responsible for the instrument and in case of loss amount as applicable will be deducted.

In the event of theft user have to lodge a FIR with the nearest police station immediately where the theft happened and approach the HR/IT Department with a copy of FIR for further necessary action

Overall System Usage Do's & Don'ts.

1. Don't give out your password to anyone, including the system administrator. It's your own and should be guarded carefully
2. Don't install any extra software on your system from external sources such as the Internet, or your personal CDs and floppies. This could have malicious code that could destroy data on your system, or even spread it to other systems on the network.
3. If you find a problem with your PC, don't try to fix it yourself. Call the support staff and lodge a complaint.
4. Shut down your system when you're leaving for the day to save power.
5. You've been given a user account and password to login to the file server. Change your password periodically. Don't make your password easy to guess.
6. Don't store your personal data such as family photos, songs or videos in your local system or on the file server.
7. In case you need to share files with somebody else on the network, then don't send it by e-mail or share your directory. Put it in the common folder on the file server, and ask the recipient to delete it after taking it.
8. Don't leave critical documents in the common folder of the file server. IT Will not be responsible for any data deletion.

Overall Network Usage Do's & Don'ts.

1. In case your system is not able to access the network, don't try to tamper with the network settings and cables. Call the IT support staff instead.
2. Trying to access areas that you're not authorized is strictly prohibited, and could have legal implications if you're caught doing it.
3. Don't send unnecessary traffic on the network, such as chain mails etc

========== End of Policy ==========