STAR
CEMENT
Solid Setting

Star Cement Limited

Information Technology Policy

Document Details

Document Title: Information Technology Policy	**Status:** Release
Prepared By & Reviewed By: G. Subramaniyam (Head-IT)	Classification: **Internal**
Reviewed on HR aspects by: Samar Banerjee (CHRO)	
Approved by: Tushar Bhajanka (MD)	Tushar

Distribution List

Version	Location
1.2	SCL, All locations

Revision History

Version	Date	Changes Made
1.2	10.03.2023	Revised Version Created
1.1	01.04.2015	Initial Version Created

STAR CEMENT
Solid Setting

Contents

1.0 Scope & Objectives

This Policy will be applicable to all the employees, contractors, Service providers sister concern (SCL, SCML, MTEPL, MPL, NECPL, SFCL, SCNEL & SCIL, STSPL, JJSSL) of Star cement limited an agent engaged with Star cement Limited as" SCL".

This Policy applies to:

a) Company application where critical business data, information and transaction are maintained & Stored

b) SAP ERP, Network & Cloud Servers, Applications, Mobile Apps and storage where reports, files confidential information, forms, checklists, drawing etc. are stored, maintained or accessed by company employees.

This Policy ensures that:

a) Critical information systems processing functions can continue or to be resumed promptly in the event of significant disruption to normal computer and /or business operations.

b) Information processed and provided by these applications is complete and accurate.

c) Network server files and non – application data can be restored promptly.

The compliance of the policies by the individuals / employees/ users shall be the responsibility Head of Department.

2.0 Detailed policy guidelines

2.1 User creation and Access control policy

While creating users at domain level/ application level/database level a written request needs to be sent to IT Department in a specified format (attached as "User ID Creation / modification / Deletion request"), which includes module name, department, user id, role to be assigned, ID type etc. The Requirement must be clear and complete.

2.2 Internet Access policy

To provide information by supporting electronic methods of distributing information to the outside world and to access and collect useful information available on the web, SCL has made access to the internet available to employees on need basis. However, SCL excepts its users to use common courtesy, common sense and restraint when placing and accessing information on the internet.

The use of Internet is subject to the usual requirements of legal and ethical behaviour within SCL. Users should be aware that they may me subject to the laws of other States and countries or on other systems or networks. Users are responsible for ascertaining, understanding and complying with laws, rules, policies contracts and licences applicable to their particular use of internet. It Understood that:

1. Users must refrain from stating or implying that they are speaking on behalf of SCL on internet. The use of appropriate disclaimers such as that set forth below is encouraged.

   "SCL does not accept responsibility for the content of any unofficial or personal home pages. The authors of such pages are responsible of all aspects of the content of their pages"

2. SCL does not normally monitor, review, approve, encourage or endorse the content of personal pages and / or the contents/ pages being browsed by individuals.

3. Individuals must obtain permission before including the SCL logo on a personal web page. However, it is sole responsibility of the user to browse web pages within the permissible limitation as per company policy.

4. Individuals may be put to disciplinary action if they post untruthful or damaging information about any associate or the company.

5. Internet facility may not be used knowingly to download or distribute pirated software or data.

6. Any activity that causes degradation of network computing resources or otherwise is objectionable in any manner will be monitored and is prohibited. These activities include:

   a) Game playing
   b) Electronic Chatting
   c) Junk mail or "Spam" mail.
   d) Reproduction and distribution of computer viruses
   e) Accessing obscene sites
   f) Mass mail forward of jokes etc.
   g) Accessing the P2P servers
   h) Downloading any software
   i) Social media and chatting sites
   j) Stock trading software/ Website

2.3 Password Policy

a) All system level passwords must be changed on monthly basis

b) All production system level password must be part of information security administered system.

c) All user level passwords must be changed every month

d) Password must not be inserted into emails or any other electronic form of communication.

e) password should not be shared in any circumstances.

Characteristic of passwords

a) All passwords should contain at least 6-8 characters
b) All password should contain both Upper- and Lower-case characters
c) The password should not contain a common word which can be found with a bit of complexity in a dictionary, passwords having date of birth, nick names, user names etc. which could be easily guessed.

SCL shares its IT infrastructure set up with group companies. Users are required to follow and do the needful for this policy/ guideline on their own.

2.4 Information Access and Data control

Data Contained in the SCL servers at all locations and the other computer systems are property of Company and IT department is its custodians. Users who have been provided with access rights to this data whether on line or otherwise, also accept responsibility for adhering to certain principles in the use and protection data.

a) Information systems with SCL shall be used only and contain only data necessary for fulfilment of the SCL business needs.
b) This data shall be used solely for the legitimate business of the company
c) Due care shall be exercised to protect this data and information systems form unauthorised use, circulation, disclosure, alteration and destruction.
d) This data regardless of who collects or maintains it, shall be shared among those users whose responsibility require knowledge of such data.
e) Proper back up of the data and other useful information is maintained by the IT department so as to re-establish the information systems capabilities within an acceptable time frame upon loss or damage by accident, malfunction or breach of security.
f) Any user or programmer engaging in unauthorized use, disclosure, alteration, or destruction of information systems of data in violation of this pólicy shall be subject to appropriate disciplinary action including possible dismissal.

g) Programmers and any IT persons are not allowed to change any live data without prior written approval from the concerned departmental head. They are supposed to work only on the dummy database for testing the new software modules.

h) Authorised users are provided with passwords for application/ data access.

i) Back up of any data which resides in user's desktop/laptop would be responsibility of users to ensure that is properly backed up in the co-ordination with IT.

j) Any loss of data due to theft or physical damage of user's system will be responsibility of users. An equivalent amount of new system will be recovered from the employee in case of loss of IT Assets issued to employee.

2.5 Email Policy

All emails, messages (for users at corporate office, units/plants and regional offices) will reside on the web space hired for that purpose. A unique email id will be provided to the Users at SCL. SCL recognises that the hardware, software and network used by the email system are limited and therefore must be managed and constantly monitored. Use of Email facility will be restricted to the prospective users only. It is expected of the email users to use this facility to enhance the performance and productivity of the company and only for company's business needs.

The Policy endorses:

1. The number of permissible mail boxes is limited. Email ids are provided on the basis of need, critically and usage.
2. Once user views his emails, they are automatically downloaded on their respective pcs and get deleted from the mail servers after 7 days from the mail server. Roaming users who are accessing mails on webmail expected to view their email messages on a daily basis so that these do not get accumulated on the mail server. Once the data is downloaded on the local machine/system the responsibility of data back -ups rests with users. In case of system crash/virus, recovery of hard disk must be approved by head – user department and Head – IT.

3. The users should restrict their messages (along with any attachment) to 15 MB size, though this is not the limitation. They must also advice their senders to send messages below 1 MB size, as far as possible. Larger attachments will be given low priority and may even be delivered only after some time.
4. Users are expected not to open any attachment which they feel are not from a reliable source.
5. The origination of further Email attachments carrying Malicious files, Such as.txt, pdf, jpg, pit, exe, vb, scr, vbe, cmd, com, dat, htp,hta, tmp, url, etc. propagation of chain letters is strictly forbidden and will be considered an abuse of company's email system. A chain letter is an email that is sent out requiring each recipient to mail it on to a number of other people, resulting in the distribution of an infinite number of email messages.
6. Individuals must not use email for any commercial offer sites/ad sites and/or entertainment purpose. They must not subscribe to free sites where they are expected to receive daily messages and block the web space unnecessarily.
7. Access to mailbox / outlook on external network/Wi-Fi/other LAN, if required shall be approved by Head- User department and Head-IT.
8. Facilitation of official mails on smart phones/blackberry I-Phone must Have approval of highest authority at site/location and Corporate Head-HR.
9. Official mails forwarding to personal mail ID should have approval of Corporate Head-HR & MD.
10. Forwarding of emails of any employees to any employees or to higher Authorities should be avoided and in case it required it should name proper Communication or intimation should be done.

Procedures and helpful Hints

1. Sending message to groups:

a. Do not select the entire address list for inclusion in the: CC: and/or BCC: fields.

b. Send only to those people who “need to know” the information.

c. Never use the Return receipt option when sending to large groups /senior executives.

2. Keep your In-box and Sent Mail folders manageable.

a. Move your important messages to appropriate folders

b. Delete any old or unnecessary messages (especially those with attachments) in your folders on a regular basis.

c. Only save what you need.

d. Only save the most up-to-date message in a thread.

3. Security of E-mail

a. Do not say anything you would not want others, besides your correspondent, to read. E-mail messages are considered private and every attempt will be made to assure the security of the email system, however, this is not a guarantee.

b. Be aware of the potential for forged mail. If a person has acquired another individual's password, that person can pretend to be the other individual and send forged mail.

c. Be extremely careful when executing programs, you receive via e- mail, as they may contain viruses that could be dangerous to the network, servers or your computer.

Email – Privacy and Disclosure

Company name e-mail is not private. E-mail messages, files and calendars are business records. Company name reserves the right to, without prior notice and for any reason, monitor access, review, copy, delete, disclose, and distribute to any party any message sent, received, or stored on the company name email systems.

Company will make reasonable efforts to maintain the integrity and effective operation of its email systems, but users are advised that those systems should in no way be regarded as a secure medium of the communication of sensitive or confidential information.

Because of the nature and technology of email, company name can assure neither the privacy of an individual user's use of the company name email resources nor the

confidentiality of particular messages that may be created, transmitted, received or stored thereby.

Email information is occasionally visible to IT staff engaged in routine testing, maintenance and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read or disclose to others, the content of email messages.

E-mail Retention

Most email messages are a form of temporary communication and may be discarded routinely by either the sender or the recipient. However, depending on the content of the email message, it may be considered a more formal record and should be retained.

Email backups are created for the purpose of business recovery. All confidential & important Emails of users to be retained on backup storage to be kept in NAS or cloud storage.

2.6 Policy on allocation of computer/laptop/printer/ IT hardware

For any requirement of computer equipment by employee, a requisition /Indent has to be raised by concerned person and get it approved by Department Head & Head IT & Unit/Location Chief. Thereafter requisition /requirement to be approved form MD for further procurement. Thereafter the allocation of the same be done as per following policy:

1. Responsibility of procurement, allocation and record keeping will be of IT department.
2. For any new requirement of any computer equipment by any user, first the possibility of allocating it from the current spare's stocks, if any, will be explored. If any item (nearest to the desired configuration) is available in the current stock, it will be allocated against the requirement.

Eligibility of Laptop allocation is Manager (M4) and above. For employees below Manager (Role based), laptop allocations can be done on business needs on special approval by

Department Head & Function Head/Unit Head, Head-HR & MD as applicable. Configuration of PCs will be contemporary.

A Desktop/laptop can be eligible for replacement after a period of 5 years of allocation. However, in case of any performance issues and provided a valid business reason is given, it can be replaced before 5 years with proper approval process.

2.7 Disaster Recovery Policy

Keep the reliable data backup as a regular routine process for preventive maintenance and system care

Using a reliable backup system, for example DAT/Tape drive solutions, CD writing, RAID 5 disk mirroring, tape cartridges etc. are used as high capacity storage devices. When backups fail, a low level read is generated in order to create a working copy of data. This policy is in place to make sure the original data is never compromised in any circumstances.

Anti-virus software and firewalls are activated for detecting malicious activities

Use reliable and reputed Antivirus Software and ensure continuous updating of the software virus definitions. Check all incoming data for viruses and this includes packaged software prior to loading them onto system. Antivirus software roll-outs/installations must be done by a technical IT consultant or experienced person. By doing standard installations one has to ensure that all incoming email is properly scanned before downloading.

It is recommended when using tape cartridges backups/disk backups, that the tapes are not re-used for longer than six months. Database Backups to be kept in Vault Securely backed up in external HDD'S.

2.8 Firewall Administration Policy

All firewalls must meet the following configuration standards:

1. Firewalls must use authentication for administrative access.

2. All firewalls shall be monitored and audited regularly to detect intrusions or abuse.

3. All firewalls must be implemented on systems containing operating system builds that have been stripped down and hardened for security applications.

4. All appropriate operating system patches must be applied to all firewall systems before any installation of firewall components.

5. All firewalls rule sets will be subject to periodic review.

2.9 Prevention Policy for Virus

1. Regular backup of data files.
2. Create and maintain strong antivirus security rules & policies
3. Install antivirus software on each computer system as well as on the Servers. Regular scans & block of all executables, such as .exe and .zip files. Scan all incoming and outgoing spam email and attachments.
4. Scheduled regular updates of the virus definition & signature files. Also update of OS whenever new signature files are received.
5. All macro virus protection within software packages such as word or excel has been enabled.
6. Using data and program disks received from unknown sources are prohibited; scan all unknown disks before they are used.
7. Restrictions on unwanted downloads of files from Internet, to be controlled by Firewall Policies & Rules.
8. All users are to be informed of new virus and security threats. Software programs must be upgraded as required. All systems should be updated with latest OS updates

& virus signature on a regular basis. OS updates & virus signature cannot be stopped /uninstalled by a user, it should be controlled by control group policy by IT dept.

3.0 ERP Authorization Process

1. User submits "ERP User creation request" duly approved by HOD to IT department.
2. ERP Head/Power user validates user's requirements in consultation with user's HOD and sends his recommendations.

Process for ERP – Request for Change

1. User creates new RFC requirement as per standard template or in the system. SOW template is used to define RFC requirement.
2. This requirement is reviewed and validated by ERP Power user along with user.
3. RFC requirement is approved/rejected by Head-User.
4. RFC requirement feasibility analysis is done by ERP technical Leads and recommendation is given to Head-IT.
5. ERP technical lead to kick off the project/requirement.

SAP Power/Admin user

Why power/admin user – In any ERP enabled organization there has to be a power user who is single point of contact for ERP technical team for any modification/implementation. Besides, he is the single point of contact for his own functional end users, in case any, ERP application help is required.

Who can be Power/admin User -Power user is the user with advanced knowledge in ERP applications and with special permissions / roles for modules.

Power/admin user's role - He primarily works in his specific department and is available to other end users for ERP related functional help. Power users also actively participate in any ERP modification and implementation.

All users should follow the SAP SOP which will be part of the Standard IT Policy and which will govern the operational procedures to be followed by each active users of SAP. Users to be created in SAP with prior approval and data to be taken through a standard user creation template. Masters pertaining to Customers, Vendors, Item, GST to be created in SAP with prior approval to taken from SPOC and data duly filled up in Standard Data Creation Template given by MDM Team of SAP. All incidents or problems in SAP Operations users should raise it via Helpdesk Portal which will be governing medium of all day to day operations and incidents. All SAP related operations will be governed through SAP SOP & its policies which will be part of IT Policy

3.1 Virtual Private Network

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the internet to provide remote offices or individual users with secure access to their organization's network.

Do's

VPN will permit only secure and encrypted connection between a company's private network and remote user through a third-party service provider based on approval.

VPN will only permit a secure and encrypted connection between a server/PC in company's private network and remote user through a third-party service provider based on approval.

3.2 Network Port

A port is an application specific or process specific software construct serving as a communication endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. The protocols that primarily use the ports are the transport layer protocols, such as the transmission control protocol (TCP) and the user datagram protocol (UDP) of the Internet protocol suite.

Do's

1. All PC's MAC address can bind with individual port at switch

2. All open port at switch level can be defined as blind

3. Open port will be allowed only in conference room

3.3 Wireless Access Point

A wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router (via a wired network), and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Do's

1. All access points have to be secured with an access encrypted key.

2. Access point key used by external users/large user groups should be changed at every month end. Process plants WAP access key should be changed half yearly.

3. All users connected to company SSID cannot change until & unless Permitted by IT dept. For guests a separate SSID is allotted with Proper access key.

Don'ts

1. No access point should be switched on/off by users.

2. No user should try to relocate WAP.

3.4 Traffic Violation/Misuse

SCL relies heavily upon its network and ERP application to drive day-to-day operations and support employees and customers. ERP access heavily depends on Wide Area Network (WAN) to access ERP remotely and more web-based applications coming online in future, the amount of traffic crossing SCL's network will grow rapidly. If bandwidth congestion and network issues are allowed to impede, then performance of ERP application & productivity in turn suffers and the entire organization may be put at risk.

3.5 IT Assets Register

IT will maintain an asset register with the details of assets held by company. Please refer appendix I for the template.

3.6 Procurement of IT Assets

The procurement requests raised by the user department for IT assets shall be validated and recommended by IT department at the respective plant/unit.

The approval for the procurement shall be made by the existing indent's approval process

3.7 IT Assets Security

IT assets such as desktops/laptops are issued to the user upon joining the organization. Any additional assets like printer, data card for mobile connectivity are also issued based on the user's requirement subject to requisite approvals.

As per SCL's policy, it is the individual's responsibility to ensure safety of the assets issued to them from the following identified risks:

a) Physical Security – Device theft.

b) Network Security – Data theft or data altering from network intrusion or alteration of in-transit data.

c) Host Security – data theft or data altering stored locally on a laptop/desktop.

Do's and Don'ts:

- Ensure your laptop is kept secured at all times. Do not leave laptop in Unattended.
- When using the laptop in a public place, ensure that the screen contents cannot be viewed by a third party.
- Never leave your laptop logged in and unattended.
- Under no circumstances should the laptop be used for any purpose that may be considered illegal or mischievous.

- All PCs, laptops and workstations should be secured with a password protected screen saver with the automatic activation feature set at 10 minutes or by logging-off when the host will be unattended.
- Removable devices should not be kept in unattended place.
- Information kept on removable media is vulnerable and easily accessible, ensure that the media is kept secured and the data secured is protected by password.

Physical Security of Hardware

Any department, which assumes responsibility for administrative data must ensure that the computing systems housing the data are physically secured.

Areas to address include:

1. Environmental factors – the equipment should be protected from excessive heat, cold, humidity and dryness. Alarms should exist to warn of threshold being exceeded.
2. Power surges – the equipment should be protected against electrical interruptions or voltage spikes and surges.
3. Protection against smoke, fire and water damage should be accomplished with smoke detectors, fire extinguishers and air-tight computer room for containment of fire suppression gas, air filters and water sensors. Alarm tied to the company and city police departments should be installed.

4. Access controls – the equipment should be properly locked up, with no vulnerabilities from drop ceilings, raised floors or ventilation ducts. In addition, glass windows should not exist or should be opaque. A log of accesses by personnel should be kept.
5. Backups should be maintained outside of the data centre too at some safe location in fireproof cabinet meant for data safety.

3.8 Data Security

Organization's mission critical business data security is of utmost importance. IT policy should ensure that all the organization's data / knowledge has been secured to the highest level.

Removable media such as pen drives, CD's, floppies and even tapes (backup/ADR/DAT/DLT tapes) can be used to illegally copy sensitive data or plant drawings etc. This can adversely impact the organization.

DO's

- CD Drive/floppy drive should be issued & installed only after proper approval.
- CD writer should be issued and installed only after proper approval.
- Usage of official pen drives should be restricted to as much as possible and should be granted only after proper approval.
- Company's mail forwarding to users on personal mail ID has to be highly restricted and will require approval of highest authority at site/location & Corporate HR Head.
- Any write activity in removal media has to be done in IT after approval of system audit nominee.

3.9 Messaging Data Security (Content & Attachment)

SCL's mail system contains very critical chain of communication/information related to business. The mail data at server level & at user level needs to be secured.

DO's

- Mail server's backup process must be implemented in order to avoid any mail data loss at server level in the event of server crash.
- Individual mail user must protect and backup their mail data to avoid any data loss in the event of system crash.

4.0 Non-disclosure Agreement & Sign-off

All the SCL's IT contract should incorporate Non-disclosure agreement,

wherever applicable like:

- FMS- Helpdesk & AMC contract
- FMS – Network contract
- Data centre contract
- ERP Outsourced Manpower contract etc.
- Mobile apps Developers, vendors & cloud data centre hosting Business WhatsApp service SMS Gateway services.

Standard Statement for Non-disclosure Agreement:

The contents of this document are aimed to be read by authorized official only. The contents of this document may not be reproduced in any form, partly or in totality, by electronic means like scanning, fax, photocopying, retyping or any other possible means without the written consent of SCL.

Any kind of financial, statistical, customer, marketing, branding, employee of any other data related to SCL's business disclosed to (vendor name) in connection with this contract, are SCL's confidential information. SCL's methodologies, products, tools and software, training materials, templates and data that may be made in connection with this contract are confidential information of SCL ("SCL Confidential Information"). All materials furnished by SCL to the vendor or its employees in any form during contract negotiation or execution would be the property of SCL and shall be promptly returned to it after completion of contract at its request, together with any copies thereof, or destroyed at SCL's request.

Any SCL's specific knowledge and business processes shall remain the intellectual property of SCL and the vendor shall not have any claim on it.

4.1 Data Card/Mobile Security

Data card is provided for connectivity to the office network while the users are outside company premises. Such facility is provided on need basis and is strictly restricted to business purpose only.

This policy includes:

- Entitlement for data card
- The procedure for the requisition of data card.

1. **Entitlement for data card**

Employees in Sr. Manager's (M4) grade and above can be issued data card provided that its business justification has been approved by user's HOD, HOD – HR (at site), HOD – IT (at site) & Site/location's highest authority.

Points to be taken care of while using data card:

- All employees have a responsibility to use data card in a professional, lawful ethical manner and for official purpose only.
- The access plans should be in accordance with HR policy.
- Internet content access should be in accordance with IT Internet Access & Content policy.

DO's

- Data card must be physically protected against their loss, damage, abuse or misuse when used (For more information, please refer to IT Assets Security Policy)
- In case of USB data cards, please use precaution while plugging the data card IN/OUT.

Don'ts

- Don't ever use data card or mobile with GPRS facility to access internet, when you are attached to SCL's network. This should be strictly complied else it will become a major security hazard to SCL's network.
- In the event of any misuse, data card facility/mobile with GPRS facility will be immediately revoked and reported to Head IT and Corporate Head HR.

4.2 USB based storage Media/CD/DVD RW/PEN DRIVES/EXTERNAL HDD

The use of personal external storage media in the SCL's system is restricted. The use of USB based pen drive / hard disk and CD/DVD media are allowed only for the purpose of taking backup of critical information or software. The usage of external media can be permitted only after approval from concerned function's HOD and HOD IT. Any external media from

vendor/customer should go through the virus scanning process in IT department before it is used in SCL's network.

Do's:

- Media should only be used to store and share information that is required for a specific business purpose.
- Media must be physically protected against any loss, damage, abuse or misuse when used (for more information, please refer to IT Asset Policy)
- The employees must handle CD ROM, Pen drives/HDD etc. in a responsible manner.
- Users should keep important files in the specific folders created at the time of issue by IT department for automated backup in the backup server.

Don'ts:

- No personal external media or storage devices should be used in office; confidential Organization data.
- Never place sensitive data on media without authorization;

- Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner;
- Any software installation on PC/Laptop will be facilitated by IT department only on IT network, users are not authorized to install the same by their own.
- Don't keep any audio, video, pictures file etc. in automated backup folder. These files are excluded from automated backup system.

4.3 Secure conversation/other collaboration tools

Chat engines/messengers will be strictly prohibited and access shall be granted rarely on approval of highest authority at site/location and Corporate Head HR.

4.4 File Transfer Protocol (FTP)

FTP (File Transfer Protocol) is used to exchange or share documents over a computer network such as internet, intranet etc. FTP to be used by specific user Name & password

Do's:

- FTP should only be used to share documents meant for official purposes only. No personal data is allowed to be kept in FTP.
- Ensure your FTP password is secured. Dictionary words are not secured. A random mix of numbers and letters is the most secured.
- Keep your password safe and secured.

Don'ts:

- Never place sensitive data on FTP server without authorization
- Don't leave data over FTP server unnecessarily and delete after its use is over.
- Never use FTP to bring executable programs which is not authorized as per SCL's IT policy.

- Any data placed on the FTP server should be first scanned with an approved and updated anti-virus and malware scanner.

4.5 Policies for new employee joining / exiting

Following policy is applicable to a new as well as separating employee:

- The computer will be allotted to a new employee based upon his/her HOD's approval and the computer's availability in the respective department.
- The new employee will be provided new ADS logon, mail id, ERP ID (if required), Internet access based upon role and HOD's and other concerned authority's approval.

- In the event of resignation of an employee, his/her computer/laptop/printer should be surrendered to IT department. Employee's mail should be handed over as per the instruction of the respective HOD. As soon as Employee's resignation is accepted by Reporting Manager/HOD/Locationwise HR employee's AD login, Mail id, ERP ID, SFA ID for Sales Team, Restricted Internet Access, Offical Data on respective Laptop/Desktop should be allowed with restrictive access with intimation to employee as well as to Reporting Manager/HOD/HR Team. All access and credential will be blocked by same day while handing over IT Assets & signing of Final No Due Certificate. Final No Due Certificate to be signed by employee and a copy to be kept in IT & HR.

4.6 IT Forms

IT Forms are standard IT templates meant to cater various IT requirements or services as per IT Industry's best business practices.

Various forms have been designed and embedded in IT Policy, wherever applicable. These forms are in line with ITIL practices which will help
standardizing IT services across SCL locations.

Do's:

All IT service request should be submitted only in standard IT template as per IT policy.

Don'ts:

No IT service request should be entertained, if it does not come in standard template.

4.7 IT Security Policy

1. This policy ensures that no authorized users can access domain and also reject the unauthorized access of USB mass storage device, Pen Drives, Mobile, CD Drives etc. The policy also ensures that no user can install or de-install any application installed in the system. No user can install hardware equipment's, drivers and stop installation of un- authorized software at client level computers. This policy also ensures that user cannot make any changes in the system file / data.
2. To block unauthorized use of pen drive or any storage media, IT will create a policy in Active Directory or through Anti-virus software and this policy will be applied to each and every computer in the network.
3. Only the approved request shall get the access of Windows Media Player, Power DVD & VLC media player or similar kind of video view Software, in case it is required to meet business requirement. Duly approved by respective HOD of concerned dept.
4. To block the internet access and also to block the unauthorized use of any restricted site like game site, movie site, music site, porn site, fraud site etc.

4.8 Data Centre Access Security

Introduction:

SCL's data centre / server room should be equipped with security access, fire alarms/suppression, water alarms, temperature alarms, UPS and Precision ACs.

Do's

- SCL's data centre / server room is a restricted area requiring a much greater level of access control. Only those individuals who are expressly authorized to enter data centre, should enter the area after entering access log sheet.
- Any forceful or improper attempt to enter data centre should be immediately reported to HOD IT / Security Head.
- The vendor's resident engineer meant for Data centre management should ensure that only authorized person enters data centre.
- Controlling access is granted to people who have free access authority into the data centre as defined by HOD IT. Controlling access is granted to SCL's core technical staff whose jobs & responsibilities require that they have access to the area.
- These individuals also have the authority to grant temporary access to the data centre and to enable others to enter and leave the data centre. People with controlling access are responsible for the security of the area and for any individuals that they allow into the data centre.
- The doors of data centre must remain locked at all times.
- Only authorized person shall have the access of data centre keys. It will be the (Data centre officer) DCO's responsibility to ensure that all data centre at site are properly locked before leaving the office premises after closing of office hours.
- SCL will enhance the access control doors to automatic through smart card ID.
- Any individual attempt to bypass the access control system will be liable for disciplinary action.
- Data centre is manned during normal office hours.

4.9 Server Access Security

- All the servers should be password protected. Which will not be common.
- The administrator should not share user id and password with anyone.
- Change the server password on quarterly basis.

- Passwords must be made up of a mixture of lower-case (small) letters, upper case (capital) letters, numbers and at least one special character.
- Select long passwords (not less than 8 characters) as the time and effort required to crack a long password is higher than that is required for breaking a shorter password.
- Before entering user id and password, make sure no one is watching you to avoid the so called 'shoulder-surfing' technique.
- Server password should be kept in a sealed envelope with infrastructure supervisor.
- Server log should be saved in a designated file on regular basis.
- All security related logs must be kept online for a minimum period of 1 week.
- All required security must be enabled for SCL's servers.
- Daily incremental tape backups will be retained for at least one month.
- Weekly full tape backups of logs will be retained for at least one month.
- Monthly full backup will be retained for a minimum of 1 year.
- Offline backup of ERP servers will be taken quarterly.
- Operating system configuration should be in accordance with approved SCL guidelines and followed.
- Services and applications that are not required, must be disabled.
- All latest security patches must be installed after due diligence and testing on all the servers.

5.0 Server security from any possible threats

The main threat to servers will be from viruses. The virus will continue to be a very serious threat to critical business data and will continue to evolve, becoming more sophisticated, dangerous and devastating.

Do's:

1. Regularly update the Anti-virus/Trojan/Endpoint software through centralized Antivirus Console automatic updates. The updates must be scheduled on a regular

basis to ensure that the software detects the latest viruses/Trojans/Worms/Malware/Ransomware.

2. Scan (full system scan) your system at least once per week with your default AV scanner software. Be sure to update the virus signature before doing so and also consider automating the process by scheduling a full system scan for convenient regular scanning in future.
3. Blocking of external storage devices e.g. External HDD, USB Devices, Card Readers should be done through Centralised Antivirus Console Rules & Policies

Don'ts:

1. Do not run any file without scanning them, no matter what the file extension is (i.e. .exe, .bat, .com, .doc etc.)
2. Freeware or any other type of software, obtained or downloaded from unknown or untrustworthy sources could easily affect company security, exposing critical business data and/or corrupting sensitive ones, hence it should not be installed.

3. Installation of any unauthorized software on any of the company work station(s).
4. Unauthorised remote desktop on servers should not be allowed.IT should be allowed only to core IT team with due permission from HOD IT.
5. Unauthorised access of external storage devices not to be done. Users to take access permission approval from respective HOD's incase of official transaction requirement.

5.1 Data backup security

Proper backup procedure will be followed for security & safety of our data and software, database (data files and control files), application executable whenever changes are incorporated and source code whenever changes are incorporated on daily basis. To take care of disaster situation early, latest monthly data backup and up-to-date application software backup is being kept at another place also in addition to regular place in data centre.

1. Backups are scheduled on daily, monthly and yearly basis in two sets and checked by IT from time to time.
2. We will use reliable backup systems, for example DAT solutions, CD writing, RAID NAS, Storage etc.
3. The server database backup (data files and control files) on a daily basis on CD/DAT/Disk Backup and its access must be restricted from users.
4. The backup of application executable files whenever changes are incorporated.
5. The backup of source code whenever changes are incorporated.
6. At least server backup would be available for last seven days [Sunday to Saturday in rotation] at any given instant on CD/DAT/Disk Backup as well as other PC which will be restricted from user.
7. The backup units are located in secured facilities and access is assigned only to IT department personnel who have a role-based need, which requires access to the facility. No other personnel have unescorted access to this facility.
8. While changes have been occurred in a source code then IT will comment current logic in the program then make a copy of source code and then only make necessary logic/syntax correction in the source code.
9. VM Backup should be taken on a quarterly basis and it should be kept in NAS storage.
10. Proper Backup Software should be implemented to take data backups of Users, Email Data, Server Data, Databases, & VM Volume Backup for all the locations.

5.2 Server Licensing

A license is a legal instrument governing the usage or redistribution of copyright protected software. A typical software license grants an end-user permission to use one or more copies of software in ways where such a use would otherwise constitute infringement of the software publisher's exclusive rights under copyright law.

The most significant effect of this form of licensing is that, if ownership of the software remains with the software publisher, then the end user must accept the software license.

- All servers should have licensed OS installed in it with proper support pack.
- All servers should be licensed product and software installed in it.
- No freeware or unlicensed software should be installed on critical server without consulting OEM and support vendor.
- License details will be prepared and maintained by site IT department.
- License inventory to be maintained by IT dept and it should review on a quarterly Basis.

5.3 Software licensing policy

This is the policy of SCL to respect the copyright protections given to software owners by federal law and use only licensed software. It is against SCL's policy for users to copy or reproduce any licensed software on SCL's computing equipment, except as expressly permitted by the software license. Also, user shall not use unauthorized copies of software on SCL owned computers or on personal/notebook computer provided by SCL for any purpose.

The software provided by SCL for use by any employee may be used only on computing equipment as specified in the various software licenses. Specifically, all the users must:

1. Abide by all terms of the software license agreement.
2. Be aware that all computer software is protected by copyright laws unless it is explicitly labelled as public domain.
3. Do not copy software for any purpose outside those allowed in that particular software's license agreement.
4. Do not make software available for others to use or copy in violation of that software's license agreement.

5. Do not accept unlicensed software from any third party.
6. Do not install, nor direct others to install, illegal copies of computer software or unlicensed software on to any SCL owned or operated computer system.

5.4 Software Change Policy

For any software change (change in business logic, enhancements, report format modification, upgradation etc.), a written request to be sent to IT department in a specific format. The user must clearly mention the application requiring change, nature of change desired (new requirement or modification), the priority, detailed specifications, impact of the change, locations where changes are to be implemented etc. and must attach the sample format. The specifications must be clear and complete. The employee making the request must get it approved by the HOD before forwarding it to the IT department. IT department will review the request and may carry out discussions with the users. The modifications are then carried out by IT department and subsequent activities take place as per the following guidelines:

1. No software change is to be carried out on verbal communication. A written request must be available for making any software change (unless it is some kind of virus fixing or temporary query). Request through mail attaching scanned copy of filled in request form template will also suffice.
2. After development is over, IT department will carry out testing on test data and will inform concerned user to test the same and provide their feedback & UAT to IT department.
3. After incorporating changes, if any, IT department will release the module to the users and will provide the handholding support/training.
4. Version control will be done by IT department.

5.4 Change Management

1. While modifying any changes at application level a written request shall be sent to IT department in a specific format (object development / Modification Request, Development ID, Prioritization of changes, change request closure timeline (due date), Impact analysis, Emergency change, Input requirements, Process requirements etc. The specifications must be clear and complete.)
2. After signing the Object development / modification request, IT will comment the current source logic by mentioning the date, description in the source code and then make necessary correction in the source logic.
3. After successful completion of changes desired, IT department will send the request to concerned department to test the modification done by IT and if correction meets the user's requirement then signed UAT form will be required by IT department to close the issue. The form will be kept by the IT department duly signed by authorized department Head, who have raised development / modification request to IT department.

5.6 Maintenance of IT Resources

IT will strive to provide uninterrupted services and to achieve this goal, IT will to adopt the following:

1. To avoid hardware failure and provide uninterrupted services to the users, IT will provide assets on Annual Maintenance Contract (AMC) for maintenance of IT assets. It will be procured as per procedure laid down for ÄMC Terms & Condition.
2. Ensure by IT In-charge that the hardware calls must be attended immediately.
3. Record of all issues reported, attended and action taken.
4. Preventive maintenance of IT equipment's must be enforced and adhered as per agree SLA of AMC.

SCL will procure and deploy widely acclaimed Service desk Management software which will be centrally managed. SCL will also deploy advanced NMS tools to centrally manage the whole network.

Annual Maintenance Contract (AMC)

To avoid hardware failure and provide uninterrupted services to the users, SCL will adopt AMC support for all IT assets as per management's direction and Facility Management Services (FMS) for any IT related support issues. The scope will be as per detailed SOW document along with RFP or Maintenance Contract.

5.7 Enforcement Authority

This policy shall be implemented by the respective Head – IT along with the help of the user department.

5.8 Change Authority

Head – IT shall make every endeavour to keep sourcing information regarding amendments to all clauses mentioned in this policy as and when they are made enforceable.

Changes to this policy shall be put up to office of MD for their approval.

5.9 Deviation from policy – procedure and approvals required

In general, no deviation from this policy is allowed. In case any deviation is sought, a detailed reasoning is to be prepared and submitted to Head – IT, upon perusal, the deviation can be allowed or disallowed.

All significant deviations made shall be reported to MD on a quarterly basis.

Appendix I

1. IT Asset Register

SL NO	LOCATION NAME	COMPANY NAME	STATUS	EMPLOYEE NAME	COMVAULT BACKUP	MSO ORIGINAL	OS ORIGINAL	DEPT.	HOST NAME	IP ADDRESS

Appendix - II

6.1 SAP User Creation & Allocation in Production

Sr.no	SAP ID	EMP Code	Name	Department	SAP Module	Locatio	Designn	Mail ID	Contact No	Type of User	Company	PLANT Code	Co Code	Job Desc	Role Name

EMAIL ID CREATION TEMPLATE

S#	Emp Code	First Name	Last Name	Dept	Designation	E-MailID	Phone Number	Location	Group Name