IT SECURITY POLICY

INDEX

INTRODUCTION & PURPOSE

- It is the intent of this policy to establish guidelines for the employees using the Company's computing facilities, including computer hardware, printers, fax machines, voice-mail, software, Business Applications(SAP-Oracle etc) e-mail, and Internet and intranet access, collectively called "Information Technology".
- The Company Information Security Management Manual has been developed to facilitate the implementation and clearly define Company's policies on Information Technology management.
- It provides a description of the philosophy of Information Security and a structure from which all other actions and methods will be accomplished in regard to the legislative requirements and information about significant Information Security Management impact.
- This document alone does not guarantee an effective Information Security Management system however, our people interacting with Information Security Management concepts and methods will provide a system of Information Security Management that is dynamic and will impact on improving the way we do business. It applies to those Information Security Management aspects, which the organization can control and over which it can be expected to have an influence.
- The policies specified within are consistent with those of best practice management principles. They have the full support and commitment of Company management and the management team approves all concepts and principles in this manual.
- IT Manual will be updated on required basis, if there are changes in the IT systems and procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome. This should be provided by email.
- The concepts contained herein are practical ideas and explanations of how **Company manages** Information Security Management Aspect.

2.0 SCOPE

- These policies and procedures apply to premises, computers, Server network and Operating systems which are part of Company and related entities.
- The purpose of this policy is to document and maintain the appropriate rules / policy to avoid confidentiality, integrity and availability related issues for changed software & hardware. These rules are in place to protect the employee and company in totality.
- The information security management shall include the IT policies such as access control to premises and operating system, automatic lockout and password protection policy, back-up policy, Business Application (Control Like UAT, Change Management etc) CD writing and data copy policy, internet policy, policy on IT server room, policy on external service provider for IT, Software and Hardware maintenance, Disaster Recovery and Management Plan.

3.0 DEFINITION

- Access – The ability to read, writes, modify, or communicate data/information or otherwise use any system resource.
- Access Controls – rules for limiting access to safeguard systems and data at all times and under all conditions.
- CIO – The CIO of the company and the person responsible for all information resources within the company.
- Employee – Individuals employed on a temporary or permanent basis by Company ; as well as consultants, contractors, contractor's employees, volunteers, and individuals who are determined by the Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the Company network.
- Information Resources – A collection of manual and automated components, each managing a specific data set or information resource.

- Interoperability – The ability of a system to use the parts or equipment of another system.
- Archive – (1) A long-term storage media, often on magnetic tape, for backup copies of files or files that are no longer in active use. (2) To move data to a less accessible or less expensive storage media or method.
- Authentication - Authentication refers to the verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and/or data.
- Authorized Network Users – Individuals who have been granted access to Company network resources through an assigned user Id.
- Backup - To copy files from one storage area, especially a hard disk, to another to prevent their loss in case of a disk failure.
- Back-up Files – Electronic files created to restore computer system files that have become inaccessible on a computer system.
- Bandwidth - A measure of the amount of data that can be passed by a communication channel in a given amount of time.
- Basic Input/ Output System (BIOS) – A set of instructions and routines that enable the computer to communicate with the various devices in the system, such as memory, disk drives, keyboard, monitor, printer, and communication ports. The BIOS handles the flow of data between the operating system and the hardware.
- Biometrics - A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).
- Central Processing Unit (CPU) – The part of a computer that interprets and executes instructions.

- Computing Resources – computer hardware, servers, PC's, workstations, terminals, printers, and other equipment physically located within the Sutlej.
- Confidential Information – All information not in the public domain.
- Configuration Files - These files contain special commands, which set up the computer's hardware components and load the device drivers (e.g., memory, mouse, printer) so the applications can use them.
- Database - An organized collection of information that can be searched, retrieved, changed, and sorted using a collection of programs known as a database management system.
- E-mail – Any message sent electronically through one or more computers and/or communications networks, and in most cases has a human originator and receiver.
- E-mail System – A service that sends messages on computers via local or global networks. Email systems provide for storage, and later retrieval of messages and attachments, as well as real-time communication.

4.0 RESPOSBILTIES

- Company is responsible for establishing and coordinating information security management policies. The final authority for this policy execution lies with the CIO.
- Under certain limited conditions, CEO/CFO/Plant Head/CIO is authorized to set emergency temporary policies, which will take effect immediately.
- The operations unit for administration is responsible for communicating IT policies to all Company employees by verbal or through Employee portal .
- IT Team shall be responsible to maintain the system in compliance with the applicable regulations.
- IT department is responsible for reviewing policies with all newly transferred and/or hired employees and also responsible for abiding all IT policies.
- IT person is responsible for posting and maintaining all IT policies and approved policies remain in effect and any modified or temporary policy that materially

affects the usage rights or responsibilities of employees will be communicated to employees by an email message alert.

- Any employee may request or suggest a new IT policy or a revision to an existing policy.

Users of information resources are responsible for the following:

- Using data only for purposes specified by the owner, complying with security measures specified by the owner and protecting the data from unauthorized access and reporting
- Information security information violations to the owner and concealing information in the data or the access controls over the data unless specifically authorized in writing by the owner.

5.0 ACCESS POLICY IT

5.1 Organisation Structure

Data Centre	Pooled Functional Resources
Corporate IT	CIO -Head IT, DGM/AGM and Manager Corporate IT
Local IT	Local IT Heads
IT Approvals & Policy Committee for Business process change	CEO /CFO / Executive President /Corp. Commercial Head/ Sr. VP / Corporate IT Head
IT Steering Committee	President, CFO ,Corporate Commercial Head /Sr. VP and Corporate IT head
For Routine issue	Local IT head. Core team, BPO

5.2 Technical and functional Structure for IT

Sr No.	Access Type	Authorized Persons	Remarks
1	Sec. Officer and CIO	Corporate IT Head	At present Mr. Vipin Shotriya
2	Sec. Administrator with All Objects	Server Administrator	At present Mr. Vipin Shotriya /Mr. C.S. Vyas/Mr. Mahesh sharma/ Mr. Avadhesh Sharma /Mr. Vijay Jangir
3	Sec. Administrator without All Objects	Site Administrator	At present , CTM-Mr. M.D Sharma, BTM 1-Mr. Jasvinder Sohal, DGHT-Mr. Chetan Mumbai Office -Mr. Mahesh Achari BTM2. –vacant
4	All Objects	Corporate IT Key Personnel	Mr. Mahesh Sharma, Mr. Avadesh Sharma ,
5	Basis Support	Basis administrator	Mr. C.S.vyas,
6	Job and Spool Control	IT Site Administrators and DC	
7	Backup	Corporate IT	Data center team Mr. Parth /Kuldeep/Ashwini/CSvyas/ Vijay Jangir
8	System on/off	Corporate IT	Mr. Vipin Shotriya /CSVYAS/Vijay jangid
9	Compilation and transportation in Production Server	Basis Administrator	Mr. C.S.Vyas
10	Server and DC Key tasks	DC Key Personnel	Mr. Vipin Shotriya /Mr. Mahesh Sharma/Mr. Avadhesh Sharma/Mr. C.S.Vyas /Mr. Vijay Jangir

11	Network/VPN/System Security /Cyber security/Email /CCTV	Network administration	Mr. Vijay Jangid/Mr. C.S vyas /Mr. Mahech Achari
12	Helpdesk for VPN/	24 X 7 Support desk	Mr.Parth/Mr. Ashwin/Mr. Kuldeep
13	HR-Payroll /Web Sites /and Others	Corporate IT	Mr. Pankaj Toshniwal /Ashwin
14	D.R. Drill	Corporate IT	Mr. C.S. Vyas, Mr. Vijay Jangir, Mr. Avadhesh Sharma, Mr. Mahesh Sharma, Mr. M.D. Sharma

5.3 Physical Premises Access Control Rules and server room

- Company maintains the strict compliance to the premise access to server room . All the servers should be kept in server room with proper cooling and power supply . Access to server room should be restricted to authorized personal from Corporate IT Team only with help of door lock . The Movement of personnel inside the data center should be recorded. The purpose of this policy is to ensure a minimum level of security is maintained by all Company staff that has access to the IT Server Rooms.
- Company Plant Head or delegated personnel are responsible to ensure that this policy is enforced and complied with. IT personnel and Office Administrator is responsible for holding and maintaining the IT Server Room Access Log.
- All staff must be aware of this policy and their obligations therein. It is their responsibility to ensure they carry out their duties in a professional manner whilst working in the IT Server Rooms.
- All visitors need to be made aware of this policy and their obligations therein. It is the responsibility of the Company member of accompanying the visitor to ensure they carry out their duties in a professional manner whilst working in the IT Server Room.

- IT head Company Plant Head or delegated personnel shall document and maintain the list of authorized person for Server Rooms Access. The IT server room will have restricted access and shall be locked appropriately.
- Access to IT server room is strictly prohibited for Visitors, unless it is for facility review, audit or inspection
- All visitors must also be recorded in the IT Server Rooms Access Log/ Register.
- The use of mobile phones, pagers or other equipment that emits radio waves within the IT Server Room is forbidden unless specific exemption is obtained from the Head of IT. Food and drink must not be taken into the Server Room.
- All relevant staff will have this policy brought to their attention by the Company Plant Head or delegated personnel. Any queries regarding this document will be dealt with by the Company Plant Head or delegated personnel.
- Unauthorized access to the IT Server Rooms must be reported to the Company Plant Head or delegated personnel.

5.4 Computer System/ Operating System & Folder Access

- Company Office Administrator/HOD shall request IT personnel to create secure and unique user id and password to operate the computer system for each employee working within Sutlej .
- HOD or office administrator shall authorize the rights of new employee for operating system access within Sutlej No additional folder rights shall be given to any employee working in company which is not granted by HOD or delegated personnel. The appropriate records for the Operating System Access rights shall be maintained by the IT department.
- Information access restriction shall be done appropriately to prevent the unauthorized access by Company employee. This shall be done through the project specific rights, folder specific rights, read only rights to the Company employee.

- Each employee within the Company shall change the password of their respective computer system as per the password policy to prevent possible unauthorized access. This shall be documented appropriately, if required.
- IT personnel shall maintain the computer system of each employee and maintain the record for any up gradation or change in operating system. This shall include the appropriate setting of features like Session time-out, Limitation of connection time, Password change reminder etc.
- IT Personnel shall check the system utility of each Company employee on required basis as directed by HOD or delegated personnel.
- IT Head unit shall ensure that the sensitive information is kept in secure and separate folder with limited access only to the authorized Company personnel.
- Personal Laptop is strictly prohibited in the premises. Please do not try to connect laptop, blue tooth, pen drive or any electronic device to this network. The Employee should not carry external media like floppies, CD/DVD's, External HDD in the premise within SUTLEJ , unless authorized by UNIT Head/Sr VP.
- The list of specification and all the records that are preserved in soft copy are kept securely by password protection and backed up regularly to prevent loss of data.

5.5 Company Email Access

- E-mail is provided to employees in order to facilitate the execution of their daily official duties and responsibilities. Use of Sutlej Group E-mail id is only for business purposes. Employee are expected to adhere following SOP and rules for use of allotted email Id by the company.
- Use of e-mail IDs for personal purposes is strictly prohibited. In case if it is required then it should have the approval of Location/ Plant Head.
- Sending of business related data by the employees to their personal e-mail ID is s strictly prohibited as this is considered a breach of Information Security. Auto forwarding of official E-mails G-suite Application to personal e-mail IDs is not allowed.

- Sending of e-mails containing defamatory, offensive, racist, anti-national or obscene remarks, pornography or any other objectionable material (including games, screen savers, .jpg or .wav or .mp3 or .scr or .bin or .zip files or other software and shareware) is prohibited and must be reported to the Reporting Manager by the Location/ Plant IT Team.

- Sending/forwarding unsolicited e-mail messages or chain mails is prohibited.

- Sending business sensitive, corporate or customer data to the unauthorized recipients is prohibited.

- The e-mails received from unknown users should not be opened and should be forwarded to Location/ Plant IT Team for verification.

- The users are responsible for keeping the passwords of their e-mail accounts confidential and must not disclose them to other personnel unless needed for work exigencies and authorized by the Reporting Manager/HOD.

- Deletion of Important e-mails related to the business is prohibited. Such action is considered as detrimental to the business and necessary disciplinary action would be taken. All users are expected to maintain back up of emails in "Local" mode with the help of IT department.

- For sending mass e-mails on "-All Users" e-mail ID, the respective users will be duly authorized by competent Authorities.

- All policy/guidelines with regard to e-mail usage are also applicable to any user, who uses mobile/ I pad devices to access official e-mails on handsets.

- The mailbox size limit has been defined for users as per the business requirements. The users should ensure that their mailbox size is within the identified limits otherwise they will not be able to send or receive mails. In case of problems, user should contact the Location IT/ Plant

Mailbox Size:10 GB – All Users More than 30 GB: As per business requirements – Business Heads and Management	Attachment limit: For All Users 10 MB – Outgoing for External mails. More than 10 MB, as per specific business requirements.

- New Email ID will be created by Corporate IT on requisition received from Plant IT; provided it is recommended by Local HR/HOD.
  The e-mail ID of a permanent employee is created in the format as under:
  <First name><Last name>@<domain name>.com or the initials used by individuals. Ranjan Kumar would be "ranjankumar@sutlejtextiles.com "
  Similarly, A. K Buxi would be akbuxi@sutlejtextiles.com

- The duplication of e-mail ID's is not permitted. A unique e-mail ID is assigned to each user. Multiple ids for single user are not permitted without prior approval of The President.
  e.g. If xyz@sutlejtextiles.com already exists; then the new ID with xyz1@sutlejtextiles.com will be created and likewise xyz2.....

- The e-mail ID of the resigned/terminated employees should be deleted or forwarded as per advice of respective HODs and Local HR. Local IT department should immediately stop email ID of resigned or terminated employees on last day of services with the company at closing working hours. Forwarding of incoming emails will be for a maximum period of 3 months. The Location IT Head should send requisite communication on the subject to Corporate IT Team.
- Company has email id of each employee in the name of Company domain.
- IT personnel shall take care of the user specific email id within the Company domain after the permission authorized by Company Plant Head or the delegated personnel.
- Each employee within the Company shall change the password of their respective email ID periodically or as required.
- Each project conducted at Company shall have unique project specific ID in Company domain and this have access only to the concerned project team. Project team shall be responsible to maintain the project specific account for project communication.
- At the end of employment, all concerned rights shall be cancelled for Company employee to access email within Company domain. Only Company Plant Head shall have rights to access the cancelled email ID to check the important email of ex-employee, if required.

6.0 Information Technology Disaster Recovery And Data Backup Policy

6.1 BACK UP POLICY

- The purpose of this policy is to provide guideline about creating back up of existing information in removable media or computers and trace the incident and make sure person doesn't violate any IT policy knowingly / unknowingly and also to maintain the integrity and availability of information and information processing facilities. These rules are in place to protect the employee and company in totality.
- Company shall maintain the back-up of server on regular basis as decided by the management i.e Daily, Monthly and yearly .
- Back-up shall be stored at different storage device other than server As per the auto back-up system, the auto back-up shall be processed on hourly basis in the internal drives, while at the end of day one more back up shall be processed in external drive.
- Restoring data/software once in a year from the backup copies should be undertaken to ensure that they can be relied upon for use in an emergency.
- DC key personnel shall ensure that the back-up is being done as per the set frequency.
- IT personnel shall maintain the back-up device in secure location within company to prevent unauthorized access. IT personnel also ensure that the back-up device is virus.
- Free and bad sectors. In case any virus is found during scan, then it should be immediately repaired or replaced as it may not be the safe media to take back-up Daily backup will keep in small fire proof rack and monthly backup will stored in main fire proof Rack with label . Yearly backup will stored in bank locker ..
- IT Personnel/ vendor shall verify the restoration of data on periodic basis to ensure the functioning of the data restoration once in a year.

6.2 DISASTER RECOVERY POLICY

- Best Practice Disaster Recovery Procedures. A disaster recovery plan can be defined as the ongoing process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

- For High availability of system New server as D.R. Server to be installed at other location after full implementation of ERP . Data center team will ensure proper replication of the main server data on D.R. server and periodically shifting the working.

- To prevent data loss for any disaster incident Sutlej installed D.R. Recovery server at Baddi location and using data replication software for data replication.

- Company have configured real time replication of complete data (All the Program, Database etc.) through MPLS 0 VPN or Secured Internet connection.

- DR drill should performed once in a year i.e to use D.R. server instead of production server during this period.

- Old Tape which are not working and 9 year old should destroyed with approval .

6.3 Incident Management Policy

- Policy

  The purpose of the incident management policy is to provide organization-wide guidance to employees on proper response to, and efficient and timely reporting of, computer security related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure, Server Failure, Network Failure etc. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within Sutlej IT.

- Scope

The organizational management shall ensure that:

1. Incidents are detected as soon as possible and properly reported.
2. Incidents are handled by appropriate authorized personnel with 'skilled' backup as required.
3. Incidents are properly recorded and documented.
4. The full extent and implications relating to an incident are understood.
5. Incidents are dealt with in a timely manner and service(s) restored as soon as possible.
6. Similar incidents will not recur.
7. Any weaknesses in procedures or policies are identified and addressed.
8. All incidents shall be analyzed and reported to the designated officer(s).
9. Learning from the incidents is recorded.

Incident Type	Responsibility
Power Failure	Mr. Vijay Jangir/Mr. Parth/Mr. Kuldeep/Mr. Ashwin
Network Failure	----do---
Server Failure	Mr. C.S.Vyas/Mr. Vijay Jangir/ Mr. Avadhesh Sharma /Mr. Mahesh Sharma /Mr. Jasvinder Sohel //Mr. M.D.sharma /Mr. Mahesh Achari
Fire Incident	All team members of Corporate IT /Security Staff

- **<u>Major Incident management plan</u>**

A. **Power Failure Incident**: For uninterrupted power supply 2 Nos of UPS system have been installed at DC and DR locations with PRS system with 3-4 hours power backup.

In case of failure of both the UPS, Power supplies can be shifted to Additional UPS installed at DC and DR for others IT department Equipment's like pc and printers.

B. **Network Failure incident:** We have taken 3 Nos of Internet connection from different service providers and configured as load balancing for high availability. In case of failure it is automatically shifted to another link and monitored by Responsible person of Plant IT/Corporate IT.

C. **Server Failure incident**: For high availability of server we having the design our system per as HA and DR servers.

In case of failure of production server. We can switch over HA server as production server. and if HA server is also fail , DR server may be activated. Proper training has been imparted to responsible persons.

D. **Fire Incident**: To manage Fire incident, we have installed Smoke detector and clean agent gas sprinklers in server room with response indicators. Fire extinguishers in all area of DC and DR are also installed.

All the team members of Corporate IT and Security Team are being trained by Safety Team. Safety team also conducted Fire Drill once in a year.

7.0 SAP Application Control

7.1 SAP Change Management Procedure

SAP Change requirement received from end user will be reviewed and examined in term of feasibility by the core team member and subsequently request is to be approved and forwarded to IT / Corporate IT.
Feasible change is supposed to develop on development environment by the in house either by the in-house ABAP team or the SAP Support team. User Acceptance Testing (UAT) of changes is to be performed on the testing server by the respective Core Team Member and sign-off is to be provided either over mail or through the change request form. VP – Corporate IT / Dy. General Manager – Corporate IT / AGM – Corporate IT will be authorized to provide the pre-migration approval. The BASIS team will transport the changes from quality to the production instance.

In case of emergency and in absence of basis team, on approval of VP Corp. IT these activities will be performed by DGM / AGM- Corporate IT. They will transport the request accordingly.

For direct changes, core Team Member will be authorized for changes through email or by filling the 'Change Request Form (CRF)', and will forward the same to IT Head - Plant for development. VP (Corporate - IT) will allocate the change request to the in-house ABAP team or the SAP support team. The change is to be performed directly to the production instance (Client: 500/544) by the BASIS team. User Acceptance Testing (UAT) of changes will be performed on the development instance by the respective Core Team Member and sign-off is to be provided either over mail or through the CRF.

For patch change / uploading for System related change, VP-IT will be the approving authority and for application related changes same as above procedure.

Any changes due to any new configuration and global policy / legal mitigation imposed by the Central / State Government for all the locations will be approved by Sr. V.P. or VP Corporate IT.

7.2 User Access Management (SAP)

User Id Creation

HOD shall request IT department to create SAP users ID Name / Generic through Email or Users creation / Modification form. Corporate IT Head approves duly requested by the IT head (Plant) will authorize the SAP application access rights of new employee with consultation with Core Team and HOD of the department.

User Access Modification.

HOD / Core team shall approve any changes in Access rights and send to IT head plant / Basis head through Email or SAP application creation / Modification form.

User Id Deletion

Generic Ids

As few generic user Ids (Shift Supervisors) may be used for SAP application and the same can be shared between more than one user. Password of Terminate / Left employee User Ids will be change by the basis team.

Named Ids

The procedure for deletion of named user Id, is as follows:
End user initiates the 'No Objection Certificate' and forwards the same to the IT department for signoff.
IT Head - Plant or VP-IT / DGM/AGM (Corporate – IT) provide the sign-off on the 'No Objection Certificate'. Post sign-off, the BASIS administrator put the validity (date of no dues) of the user Id.

Periodic user access rights review

Periodic review of user access rights is performed every year by business Head/ERP owner.

7.3 User Access (Logon Password)Policy User can access Sap application through given user Id and password only. In the event of SAP user leaving the services IT department shall change the password in case of generic ID and in case of named ID it shall be deleted. Basic principle: Give a User the minimum privileges for the shortest time necessary to do their work.
Basis team shall monitor and ensure that Users Id is used by the specific person only and no interchange of the same shall be allowed.
Password should automatically expired in every 30 days
The username should not be more than 12 characters.
Session should log out on 30 minutes of idle time. If an account is subjected to continuous login failures in short period of time (e.g. 3 attempts), block the uses ID.

7.4 Password Standards The combination of username and password define the identity of users on a system. Adopting a good personal password policy is the most important barrier to unauthorized access in current systems. Content

- **Mixture of numbers, capital letters, small letters, numbers and special Char,.**
- **Password should be 8 Characters**
- Password automatically expired in every 30 days

8.0 CD WRITING & DATA COPY

- Company office administrator shall maintain the track of documents which will be copied to CD/DVD and other electronic media. The information (type of media, information details, total MB and purpose if any) shall be documented in respective logs with prior written permission of superior authority.
- No computer in Company shall have access to the external driver/ CD/DVD driver/ USB drive, except for computer system which is authorized by Company Plant Head /Sr. VP.
- USB or required drive can be enabled only on the request of Company Plant Head for certain time frame only. Once the task is completed, copied external driver/ CD/DVD driver/ USB drive shall be taken back to maintain the confidentiality of record.

9.0 SOFTWARE AND HARDWARE MAINTENANCE

- Company IT person shall maintain the list of software and hardware installed in each operating systems and Company server.

- Company shall use the appropriate license version of SAP software and screening system to maintain the IT server set up and computer systems of employee.
- It person shall document and maintain the list of software/ hardware with their serial no, key, expiry and supplier name. License for software shall be renewed in advance before it expires by the IT Personnel, if applicable.
- Before changing to any hardware data back should be taken on removable optical drive. In case of hardware crash and data is not possible to recover then send the hardware for data recovery following the third party policy.
- In case of software repair; past data should be recover first and then run the set up file. In case data recovery is not possible before running the set up file for repair of software then during repair and running the set up file make sure that existing data should not be delete, overwrite or modified.
- Each record for the software maintenance shall be maintained complete by Office Administrator.

10. Risk Managenment

10.1 UTM (Internet / Firewall)

- Objectives In organizations which have ERP system , multi location application , large number of users and high turnover of employees , especially who are key users of ERP it is a must to protect the data and internal information of the company and the business and firewall is a must to ensure the same.

- UTM(unify threats management)/ firewall are generally proprietary system , say , Cisco series / SHOPOS etc which run on get way level Security should have strong features such as content web server protection, Ip sec tunnel, filtering , blocking unwanted hosts etc.

- SHOPOS UTM (Device) (Unify Threat Management) system at all Sutlej locations had already been implemented. It prevents, detains and filter all kind of threats at gateway level i.e. unauthorised person cannot enter into our Network and UTM also detects any viruses, spyware etc.

- Firewall Rules/Policies Internet browsing is allowed to particular users. For rest of all it is denied. For Internet users, some host groups are created like IT Admin (Full access),Sr Sr. Exec (access to Share and stock market, financial sites), Accounts (access to Financial sites, banking sites) etc. Different internet usage policy is created for all the groups according to their requirements.

  Policies are time based (Timing is scheduled), content based (unhealthy web contents/websites blocked). Gateway Antivirus and Gateway Antis spam are subscribed on firewall to detect and block Viruses and spam's at gateway level. Internet Bandwidth is limited to 4MBPS to 20 MBPS maximum for all LAN users. If the usage is below the Max limit, then remaining bandwidth will be used by WAN users connecting to SAP application.
- Policy for WAN (Internet) users Maximum availability of Internet bandwidth for Accessing SAP Application from remote locations via Internet. Only server access is allowed to users. WAN to LAN access is not allowed.
- Policy for SAP users :- Created Secured IPsec tunnel (Site to Site) for SAP users of all units in which data travel in encrypted form .
- **created SSL-VPN users for those working from home with limited permissions .**
- Log and alerts are generated and monitoring on daily basis .
- Firmware and New patches are applied by IT team periodically as per notification received form Service providers.

10.2 Anti Virus (End point Protection)

- Symantec End Point / Trend Micro apex central (anti-virus) protection for all our unit locations have been implemented. It works on Intranet network level (LAN) and prevents from virus and is also used for device control like port blocking etc.
- Created various rule for application control and device controlling for users.
- Perform auto scan of all PC and Server through End point Protection server and monitoring logs.
- New Virus/Threats definition are updated in system on daily basis.

- Information Services The Company's computer network introduces new resources and new services through Internet connectivity. This connectivity not only results in new capabilities, but also in new risks and threats. This document formally defines our official policy regarding Internet security in response to potential risks. All Internet users are expected to be familiar with and to comply with this policy. Unless specifically stated otherwise, all statements and policies will apply to both the Internet.

  The Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners and vendors) who access the Internet through the computing or networking resources.

  The company's Internet users are expected to be familiar with and to comply with this policy. Users are also required to use their common sense and exercise their good judgment while using Internet services. Connection to the Internet is almost inevitable in today's commercial environment, especially for research departments. Due to its lack of structure & controls, the Internet offers many risks such as: Disclosure of confidential information. Hackers from the Internet may penetrate the corporate network. Information may be changed or deleted. Access to systems could be denied due to system overload.

- **Unauthorized Access :-** Internet connectivity increases the risk of unauthorized access to company systems and files. The scope of this risk includes the servers supporting company connectivity as well as other systems that are connected to the same physical or logical network as these servers. Malicious activities that may result include: Disclosure of confidential information that results in loss of customer confidence, and/or legal action in situations involving customer privacy and regulatory matters. Unauthorized creation or modification of information that results in loss of data integrity. Corrupted data may also adversely affect business decisions making on financial, strategic, or competitive issues. Denial of service or operational delays due to attacks that jam or disable network

components, rendering the network unusable. This threat to the timeliness of information and information processing services may prevent the company from meeting critical deadlines and impact the quality of our products and services. Viruses introduced intentionally by a malicious individual or accidentally through files downloaded from the Internet may degrade service and system availability network-wide. They may also result in the loss or corruption of information required to maintain vital operations or support corporate-wide business decisions. Misleading or False Information All information taken off the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

- Internet Services Allowed Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will beprovided to users as needed: E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments). Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only. File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
- Only authenticated users who have been approved by the IT department for access to their internal networks will be allowed in from the Internet. All the users in the organization is having internet access, therefore the browsing access is provided to the users i.e. HTTP no FTP access is provided. Non-Company Personnel External clients or non-company personnel are not permitted access to company internal networks unless specifically approved in advance by the IT department.

10.3 Internet Usage Policy

- Use of the internet by employees of Company is permitted and encouraged where such use supports the goals and objectives of the business. However, Company has a policy for the use of the internet whereby employees must

ensure that they comply with current legislation, use the internet in an acceptable way, do not create unnecessary business risk to the company by their misuse of the internet

- Company accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.
- In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the Company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- In particular the following is deemed unacceptable use or behavior by employees:
  - `visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
  - using the computer to perpetrate any form of fraud, or software piracy .
  - using the internet to send offensive or harassing material to other users
  - hacking into unauthorized areas
  - publishing defamatory and/or knowingly false material about Company , your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
  - revealing confidential information about Company in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
  - undertaking deliberate activities that waste staff effort or networked resources

10.4 Risk Audit : Cyber Security Audit should be conducted by External Agency/Service Providers once a year .

11. MISCELLANEOUS

11.1 Operating Systems and Application Software Access Control

- All Company users must be positively identified by having a unique user-ID and a personal, secret password before being able to gain access to any computer system as verified against the security table at logon.
- The system must be able to display or report current access rights of a user showing the user-ID and all of their access capabilities to resources [e.g., file accesses, grants, permissions, etc.].
- Relevant operating system policy shall be followed for the software access given by Sponsor/ Outsourced Agency.
- Users entering new passwords shall be required to enter unique passwords. At least one of the following should be used:
  - Restrict the re-use of the last 5 passwords.
- Methods to restrict access of authorized persons should be employed after three (03) consecutive unsuccessful attempts to enter a password. At least one of the following should be used:
  - The involved user-ID must be locked/suspended.
  - The IT Administrator is required to reset the password in order for the user to be able to access the system again.
  - Continuous monitoring and alerting functions are employed to detect access failures.
- Refer to Password Policy

Physical Security:

- Application file/database servers that store application electronic records or programs within Company shall be located in controlled areas such as computer

rooms with adequate physical access security, ventilation, and protection from hazards such as fire, heat, and water.

11.2 Maintaining your PC

Computers can appear to slow down with use. Although degrading hardware (such as hard disks) can contribute, the main cause is usually incorrect, temporary and historic files or settings affecting the software.

You can prevent and reduce the effect of slowdown on your computer by performing simple maintenance.

- Reboot your computer
- Clear your temporary internet files
- Remove any unwanted files from your desktop, M: drive and departmental/section drives
- Disk maintenance is automatically performed on any computer left switched on overnight (this only needs to be performed occasionally)

11.3 Power Saving and Power backup

Computers and their monitors can use a lot of power. With each office holding multiple computers, it is very important to take appropriate steps to reduce unnecessary power consumption.

You can reduce the amount of power used by your computer by performing these simple tasks.

If you can, shut down your PC and switch off the monitor at the end of each day before you go home.

- The least amount of power a computer can use is through being switched off, so please shut down your PC and switch off the monitor if you intend to be away from it for a significant amount of time.
- If you are taking only a short break from your PC, simply lock the screen using CTRL-ALT-DEL followed by ENTER and then switch off your monitor. Switch the monitor back on and unlock your PC when you return.

- Unplug any USB peripherals that aren't in use, except for printers, as these will take power from the machine.
- Do not remove the power lead to your computer or switch off at the wall socket, as this shortens the life of the internal battery.
- Any PC or printer hardware that is unused or surplus to requirements should be reported to the Company Administration so it can be redeployed elsewhere.
- Consider not printing documents as printers use power along with toner and paper.
- Printers fitted with a duplex option (double sided printing) will be set as default to print duplex; this reduces paper wastage and saves power and users should not over write unless absolutely necessary.
- Where possible consider reducing the number of personal printers by using shared departmental printers.
- UPS should be installed for power backup / un interrupted power supply separate for server and other equipment's with proper battery backup.