The Supreme Industries Ltd (TSIL)

Information Technology System Policy Manual

Document Reference: TSIL_PO_01

Table of Content

Introduction:

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

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

Scope:

This policy governs the usage of IT infrastructures from an end user's perspective. This policy is applicable to all employees and all those who are associated with TSIL for using their infrastructure..

Objective:

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

ODBC connection to SAP carries inherent risks pertaining to security, data visibility, performance & read-locks which may result in slowing the HANA transactions. SAP strongly recommends using RFC, Web Services, OData to fetch the data.

In this context, new ODBC connections and new ODBC queries should be avoided and will be approved on exceptional justifiable grounds by the CIO office only.

Categories of Employees:

The following levels of employees are in TSIL:

- Director level
- HoD level
- Officer/Manager level
- Staff level

Type of Employment

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

1. Desktop / Laptop Devices Policy:

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

Security and Proprietary Information:

- User shall take prior approval from the competent authority of TSIL IT to connect any access device to the network.
- All active desktop computers shall be secured with a password-protection which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
- Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code. IT department will take utmost precaution to ensure that the emails & the attachment to the emails are properly scanned before they are [resented to the end user.

- Users shall properly shut down the systems before leaving the office.
- Booting from removable media shall be disabled. Use of external storage media by user shall not be allowed. Consequently all the communication ports will be disabled by the IT department. If the use of external storage is necessary, with due approval from the competent authority, the port willbe opened.
- Users shall be given an account with limited privileges on the client systems. No user shall be given administrator privileges unless deemed fit by the IT department
- If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be disconnected (by either detaching the network cable – usually grey coloured – or logging off from the WiFi network) from the network immediately and report to the IT department immediately for corrective action.

Use of software on Desktop systems:

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

Purchase of Desktop & laptop:

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

The minimum desktop specification details are as follows:

Details	Category 1	Category 2	Category 3
Processor Speed	i7	i5	i3
RAM	8 GB	8 GB	8 GB
Hard Disk	500GB	500 GB	500 GB
Operating System	Win 10 PRO	Win 10 PRO	Win 10 PRO

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

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

The minimum laptop specification details are as follows:

Details	Category 1	Category 2
Processor Speed	core i7 /i5	core i3
RAM	8 GB	8 GB
Hard Disk	500 GB	500 GB
Operating System	Win 10 PRO	Win 10 PRO
Weight	Less than 1.5 Kg	Less than 2 Kg

*** The configurations listed above is subject to change without notice.

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

Purchase of computer peripherals:

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

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

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

IT department discourages other functions from procuring IT hardware directly without the department's knowledge.

Power Connection to Computers and Peripherals:

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

Purchase of Server systems:

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

All purchases of server systems must be supported by guarantee and/or warranty of 3 / 5 years and be compatible with the TSIL requirement.

IT is highly recommended that IT department should be entrusted with the job of any server procurement due to its little complex nature.

IT Hardware Failure:

Where there is failure of any of the hardware, this must be referred to IT Associate (Hardware) immediately. It is the responsibility of IT Associate (Hardware) to assess the primary troubleshooting in the event of IT hardware failure, if the problem persists then the ticket will be escalated to the vendor.

2. Password Policy:

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

All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous 05 passwords. Password shall be enforced to be of a minimum lengthof 8 character and comprising of mix of alphabets, numbers and special characters.

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

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

Maintaining the password sanity completely rests with the user who is using the IT equipment.

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

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

Compliance:

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

3. Security Policy:

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

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

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

Keeping device secured:

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

4. Antivirus Policy:

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

Symptoms of an Infected Computer:

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

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

Deployment of Antivirus:

- For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed.
- In a networked environment, an antivirus server should be deployed and all the systems should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as updation of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.
- Identify all the possible entry points in the network through which a virus attack is possible and all the traffic entering the network through these points should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP orPOP3.
- IT department will ensure that the AV updation process is automated to maximum extent so as to have less inconvenience to the user.

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

- IT department will choose the best available anti-virus software solution. The IT department is solely responsible for AV management in the company. This may involve installing a server or using the cloud based solutions.
- For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
- For a networked environment there must be a central server or cloud based solution to check for viruses' in all the machines automatically.
- The following schedule is suggested for a full scan of the PC's.
    - Servers: Weekly
    - Workstations: Weekly

- Usually such activity is scheduled when there is less human interaction with the PC or any network device.
- The antivirus software should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engineis available.

- External media (ex. Floppy, CD's) is one of the most potent medium for transmission of viruses', hence it must not be used in the network except for afew pre-determined PC's approved by competent Authority.
- Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies of the organization.(?????)
- Unneeded services should be turned off and removed. By default, many operating systems install auxiliary services that are not critical e.g. an FTP, telnet or a web server. These services are avenues to attack, these services tobe stopped.
- Enforce a password policy. Complex password makes it difficult to crack password files on compromised systems/computers.
- Mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block/ remove attachments that are commonly used to spread viruses, i.e., .vbs, .bat, .exe, .pif, & .scr files.
- Employees must be trained not to open attachments unless they are expecting them.
- Do not allow user to execute software downloaded from internet unless certified safe by system administrator.
- In the case of a virus attack the following steps are required to be taken.
    - The network access of the machine has to be stopped
    - The contact person for cleaning the machine of virus has to be notified

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

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

Filtering and blocking of sites:

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

- Access to OTT Platforms shall be blocked across network.
- Access to social media platforms, personal emails, broking platforms, travel platforms shall be allowed where deemed fit with approval from competent authority.

Access to Wireless Networks:

To ensure information security, users are prohibited from connecting their devices to unsecured wireless networks.

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

6. E-mail Policy:

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

E-mail ID shall be provided to employees of TSIL, who need to communicate through E-mail in carrying out their duties towards attainment of the goals of TSIL.

E-mail ID shall be provided to non-employees at the discretion of TSIL, Management.

E-mail user should ensure that the E-mails are consistent with TSIL's all other policies.

All information created, sent, or received via TSIL, E-mail system including E-mail messages and electronic files, is the property of TSIL, Employees shall have no expectation of privacy regarding this information.

All the E-mails sent outside the organization shall have an appropriate Disclaimer attached as defined by the IT Department in consultation with the Legal department

TSIL, reserves its rights to:

- Deny an E-mail ID to any individual or team.
- Decide E-mail ids as per E-mail procedure.
- Access, read, review, monitor, copy, intercept, block or auto forward E-mails and files on its system for legitimate Business reasons, without prior notice.

The e-mails and electronic messages shall be protected from unauthorized access, alteration and denial of service.

Users must also abide by copyright laws, ethics rules, and other applicable laws while using TSIL, E-mail system.

Users shall exercise sound judgment when distributing messages. TSIL-related messages shall be carefully guarded and protected.

User shall not use e-mail facility for un-authorized use. Unauthorized use of email system shall mean:

- Transmitting and/ or distributing E-mail containing derogatory, inflammatory, insulting, abusive, or libelous information about any other TSIL, employee, TSIL, associate or any other person whatsoever.
- Conducting any business (whether personal or professional) via TSIL,'s E-mail system other than legitimate TSIL,'s business.
- Spamming, sending junk mail, executable files, graphics, jokes, chain mails etc.

- Enclosing information that is harmful to TSIL, or members of TSIL.
- Sending or distributing questionable E-mail containing expletives or pornography.
- E-mail users should protect others' right to confidentiality.

Use of TSIL,' E-mail system to solicit for any purpose, commercial, personal or otherwise, without the consent of the TSIL,' Management is strictly prohibited.

Mailbox not accessed for 60 days or more will be subject to blocking of the same before being cancelled.

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

Violation of this policy will subject a user to disciplinary action as per Human Resource Procedure.

7. Software Policy:

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

All software's like licensed, open source, freeware, etc. must be approved by competent authority from IT department prior to the use or purchase or download of such software.All license software must be purchased in the name of TSIL. License products like Operating System, Microsoft Office, Convertor software, Database software, etc. will be installed for the users.

It is recommended that the software required be purchased through pay per use basis rather than outright purchase.

8. External / Own device Policy:

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

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

The IT department reserves the right of installing the device management software such as MDM, etc.

Once such a software is installed in a BYOD device the policies defined in the software will supersede the policies used previously in the “official” area of the device.

Each employee who utilises personal mobile devices agrees:

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

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

9. Backup Policy:

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

Restoration rehearsals shall be conducted for all critical applications and these shall be performed once every 90 days or at frequency decided by the asset owner.

All the operations staff will be responsible for adhering to the backup norms in their day-to-day support activities for other users in the organization.