SATIA INDUSTRIES LTD

VILL.RUPANA,MUKTSAR-MALOUT ROAD,SRI MUKTSAR SAHIB

Information Technology

Policy and Procedure Manual

Table of Contents

Introduction

The SIL IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines SIL will use to administer these policies, with the correct procedure to follow.

SIL will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Technology Hardware Purchasing Policy

Policy Number: SIL-IT-HW-0001

Policy Date: 1st May,2023

Update Policy Date: 1st July,2023

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

Procedures

Purchase of Hardware

Purchasing desktop computer systems

The desktop computer systems purchased must run a windows 10 pro or latest version of and integrate with existing hardware data server AD server & Domain Server.

The desktop computer systems must be purchased as standard desktop system bundle and must be branded such as HP, Dell etc.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of 19.5" or above

- Keyboard and mouse You may like to consider stating if these are to be wireless
- Windows 10 Pro & above, and Sap GUI, Office 2016 or higher.
- such as Built in speakers, printers etc.

The minimum capacity of the desktop must be:

- I5 4.2 or Higher
- 16 Gb or Higher

- 1 Tb SSD or Higher
- Key Board & Mouse.
- USB ports.
- HDMI Port.

Any change from the above requirements must be authorised by IT Head as per the need of application/Software.

All purchases of desktops must be supported by 1-3 years warranty and renewal with care Pack 2-3 years as per availability of Parts at manufacture end and be compatible with the SIL server system.

All purchases for desktops must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing portable computer systems

The purchase of portable computer systems includes portable HDD, Pen Devices , Notebooks, Laptops, Tablets etc.

Portable computer systems purchased must run a windows 10 Pro & Higher Version and integrate with existing Data Server, AD server & Domain Server.

.

The portable computer systems purchased must be HP, Dell, Acer, etc..

The minimum capacity of the portable computer system must be:

- I5 4.2 or Higher.
- 16 Gb or Higher.
- 1 Tb SSD or Higher.
- Display 14” or Higher
- USB ports as per Model.
- C type USB Port.
- HDMI Port.

- SD card slot.

The portable computer system must include the following software provided:

- SAP GUI Application, Office 2016 & Higher, Adobe, Reader, Internet Explorer etc.

Any change from the above requirements must be authorised by IT. Head as Per need of Application.

All purchases of all portable computer systems must be supported by 1-3 years warranty & renewal with Care Pack for 2-4 Years as per availability of Parts at manufacture end and be compatible with the SIL server system.

All purchases for portable computer systems must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing server systems

Server systems can only be purchased by Purchase Department as per the need of application & Database with recommended IT specialist (Make IBM, Dell & HP).

Server systems purchased must be compatible with all other computer hardware in the business.

All purchases of server systems must be supported by minimum 3y/3y/3y (Part, onsite supports, Service) and after warranty AMC by manufacturer minimum 4 years (total support of Server Minimum 7 year) and be compatible with the business's other server systems.

Any change from the above requirements must be authorised by IT Specialist.

All purchases for server systems must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives, external pen 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.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by Department Head/IT Head or recommended IT specialist.

All purchases of computer peripherals must be supported by as per company guarantee and/or warranty minimum one Year and be compatible with the business's other hardware and software systems.

Any change from the above requirements must be authorised by IT Head.

All purchases for computer peripherals must be in line with the purchasing policy in the Financial policies and procedures manual.

Purchasing mobile telephones

A mobile phone will only be purchased once the eligibility criteria is met. Refer to the Mobile Phone Usage policy in this document.

The purchase of a mobile phone must be from Authorised Dealers/ Distributor only to ensure the business takes advantage of volume pricing based discounts provided by authorised suppliers. Such discounts should include the purchase of the phone, the phone call and internet charges etc.

The mobile phone must be compatible with the business's current hardware and software systems.

The mobile phone purchased must be Smart phone manufacturer iPhone, Samsung.

The request for accessories (a hands-free kit etc.) must be included as part of the initial request for a phone.

The purchase of a mobile phone must be approved by JMD/ ED/ MD Sir prior to purchase.

All purchases of all mobile phones must be supported by as per manufacturer guarantee and/or warranty.

All purchases for mobile phones must be in line with the purchasing policy in the Financial policies and procedures manual.

Policy for Getting Software

Policy Number: SIL/IT/SW-0002

Policy Date: 1st May,2023.

Purpose of the Policy

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

Procedures

Request for Software

All software, including {insert relevant other types of non-commercial software such as open source, freeware, etc. here} must be approved by {insert relevant job title here} prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by Purchase Department with recommendation of IT Head.

All purchased software must be purchased from reputable software Dealers/ Distributors.

All purchases of software must be supported by minimum One-Three year and AMC applicable and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by IT Specialist.

All purchases for software must be in line with the purchasing policy in the Financial policies and procedures manual.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from IT Hear/ IT Seniors must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the business’s hardware and software systems.

Policy for Use of Software

Policy Number: SIL-IT-SU-0001

Policy Date: 1st May,2023.

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licences will be followed by all employees of the business.

Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of IT Department to ensure these terms are followed.

IT department is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

IT Department is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the business's computers.

All software installation is to be carried out by IT Department.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the getting software policy is to be used within the business.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the joint responsibility of IT Department/ Department Head.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.

Unless express approval from IT Head & Department Head is obtained, software cannot be taken home and loaded on a employees' home computer

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from IT Head & Department Head is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the SIL and must be recorded on the software register by IT Department.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to HR Department for necessary action. The illegal duplication of software or other copyrighted works is not condoned within this business and HR Department is authorised to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to HR Department for necessary action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT department immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to HR department for necessary action.

Additional Policies for Use of Software

Technology Hardware Policy

Bring Your Own Device Policy

Policy Number: SIL-IT-OD-0001

Policy Date: 1st may,2023.

At SIL we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to SIL network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and Pen Drives for business purposes. All staff who use or access SIL Network/ Technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- Smart Phone allowed to Staff & Visitors only.
- Keypad Phone Allowed to some of Workers Like Security Guard, Peons and Critical areas.
- Contractor Labour not allowed any mobile devices.

Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with HR department.

If unauthorized person carrying his personal devices in the premises, then they will carry after prior permission from concern department Head and security department will record the device and all applications used by the device.

Personal mobile devices can only be used for the following business purposes:

- An unauthorised person has requirement use email access, SIL internet access, SIL telephone calls will take prior permission from concern department head.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer SIL or personal sensitive information to the device. Sensitive information includes SIL Drawing, SIL documents & other information that you consider sensitive to the SIL.
- Not to use the registered mobile device as the sole repository for SIL information. All business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that SIL 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
- To maintain the device protected with Seqrite End point Security System.
- Not to share the device with other individuals to protect the business data access through the device
- To abide by IT Department internet policy for appropriate use and access of internet sites etc.
- To notify IT Department 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 SIL equipment.

All employees who have a registered personal mobile device for business use acknowledge that the business:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device where the employee wants to sell the device

- 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

- Has the right to deregister the device for business use at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- 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.

Exemptions

This policy is mandatory unless IT Department/ Finance Department/ Legal Department grants an exemption. Any requests for exemptions from any of these directives, should be referred to the management.

Breach of this policy

Any breach of this policy will be referred to HR department who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

Indemnity

SIL bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify SIL against any and all damages, costs and expenses suffered by SIL arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by SIL.

Information Technology Security Policy

Policy Number: SIL-IT-SP-0001

Policy Date: 1st May,2023

Purpose of the Policy

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

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through keypad, locks etc.

It will be the responsibility of IT Department to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify IT Department immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the SIL laptop, notepads, iPads, mobile phones etc.. Each employee is required to use the device protected locks, passwords and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the device will assess the security measures undertaken to determine if the employee will be required to reimburse for the loss or damage.

All Desktop, Laptop, Notepads, iPads, Printer Scanner etc. when kept at the office desk is to be secured by in lock & Key provided by SIL.

Information Security

All devices relevant data to be backed up here – either general such as sensitive, valuable, or critical business data or provide a checklist of all data to be backed up is to be backed-up.

It is the responsibility of IT Department to ensure that data back-ups are conducted frequency of back-ups and the backed up data is kept on external device is to be kept offsite venue, employees home.

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

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be terminate from job.

Technology Access

Every employee will be issued with a unique identification code to access the SIL technology and will be required to set a password for access every.

Each password is to be alphanumeric and one Special Character minimum length 10. and is not to be shared with any employee within the SIL.

IT Department is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after three attempts, then IT department is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

The following table provides the authorisation of access:

Technology – Hardware/ Software	**Persons authorised for access**
All type IT Responsibility	S. Harmander Singh Sidhu (GM-IT)
FICO Module PM Module and overall maintenance/ development in SAP	Mr. Surinder Kumar, Sr.Manager(IT)
CCTV Camera, Networking, Desktop, Laptop maintenance & installation	Mr. Anmol Kanti(Asstt.) & S.Kirat Singh(Asstt.Officer)
Software Installation & Policies implement	Mr. Balram Kumar(Dy.Mgr) & Mr.Peush Sharma (Sr.Exec.)

Technology – Hardware/ Software	Persons authorised for access
Servers Installation & maintenance	Mr. Balram Kumar(Dy.Mgr) & Mr.Peush Sharma (Sr.Exec.)
SAP MM Module	Mr.Balram Kumar (Dy.Mgr)
SAP SD Module	Mr.Peush Sharma (Sr.Exec)
SAP PP & QC Module	Mr.Kirat Singh Gill
SAP Master Creation & HR Module	S.Harman Singh(Asstt)

Employees are only authorised to use SIL computers for Office use only. when this is allowable and what they can personally use it for here, such as internet usage etc..

For internet and social media usage, refer to the Human Resources Manual.

It is the responsibility of IT Head to keep all procedures for this policy up to date.

Additional Policies for Information Technology Security

Emergency Management of Information Technology Policy

Information Technology Administration Policy

Information Technology Administration Policy

Policy Number: SIL-IT-AP-0001

Policy Date: 1st May,2023.

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the business.

Procedures

All software installed and the licence information must be registered on the SIL. It is the responsibility of IT Department to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

IT Head is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by IT Head.

IT Department is responsible for maintaining adequate technology spare parts and other requirements like RAM,HDD, Pen Drive, Toners, Cartridge & printing paper etc.

A technology audit is to be conducted annually by Internal Auditors to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to Management.

Website Policy

Policy Number: SIL-IT-WP-0001

Policy Date: 1st May, 2023

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

The keeping the register up to date will be the responsibility of IT department.

Company Sectary will be responsible for any renewal of items listed in the register.

Website Content

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of Company Sectary/ CFO.

The content of the website is to be reviewed Quarterly

The following persons are authorised to make changes to the business website:

Mr. Rakesh Kumar Dhuria, Company Secretary.

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the SIL.

All data collected from the website is to adhere to the Privacy Act

IT Service Agreements Policy

Policy Number: SIL-IH-AP-0001

Policy Date: 1ST May 2023

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the SIL.

Procedures

The following IT service agreements can be entered into on behalf of the SIL:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of business software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements, obligations and renewals must be recorded in IT Department.

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by Management.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, before the renewal approval must be approved by Management. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Management

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to Legal Department who will be responsible for the settlement of such dispute.

CCTV Policy

Policy Number: SIL-CCTV-AP-0001

Policy Date: 1ST May 2023

1.1 The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system at SIL. Cameras are used to monitor activities within buildings, on its sites, bound walls, Vehicle Yard, its car parks, Motor Cycle Parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the SIL, together with its Fellows, staff, Workers and visitors.

1.2 CCTV monitoring and recording systems will only be installed in or on SIL property when this has been reviewed and approved by the SIL Management.

1.3 The system comprises a number of fixed and fully functional (Pan/Tilt/Zoom) cameras located in buildings and externally around the SIL. These are monitored by appropriate personnel.

1.4 The CCTV policy will be registered with the Information Commissioner under the terms of the Data Protection Act 2018. The SIL use of CCTV complies with the requirements of the Data Protection Act.

1.5 This policy document will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.6 The CCTV system is owned by the SIL with High regulation 4K Camera’s.

1.7 Independently installed and operated CCTV systems by staff/Workers are not permitted on any SIL property and where found actions will be taken to close these systems down.

2. OBJECTIVES

2.1 The objectives of the CCTV Policy are to: (a) Protect SIL property. (b) Ensure a safer environment within the SIL. (c) Support the Police in a bid to deter and detect crime, by providing evidence in support of an enquiry or prosecution.

3. OPERATION OF THE CCTV SYSTEM

3.1 Management of the system

3.1.1 The CCTV operating system is administered and managed by the Head Porter in accordance with the principles and objectives expressed in this SIL policy document.

3.1.2 All cameras are monitored on the respective site where they operate, but can be monitored by authorised personal on computers within the IT Department by use of the ‘CCTV Window’ programmes and by the SIL IT Department.

3.1.4 The CCTV system is operational 24 hours a day, 365 days of the year.

3.1.5 If out-of-hours emergency maintenance is required, the duty operator must contact a member of the IT in order for a call out to be authorised.

3.1.6 Emergency procedures will be used when it becomes necessary to call the Emergency Services.

4. DIGITAL RECORDING PROCEDURES

4.1 Rules for storage of data

4.1.1 In order to maintain and preserve the integrity of the Network Video Recorder (NVR), hard disks used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to.

4.1.2 Each NVR must be identified by a unique mark or serial number. This is maintained by the IT Department.

4.1.3 Each NVR must be kept in a secure location with access restricted to authorised staff.

4.1.4 The IT Seniors or on-duty person, in liaison with the IT department, shall check daily to ensure the system is operational.

5. ASSESSMENT OF THE SCHEME

5.1 Performance monitoring, including random operating checks, may be carried out by the IT Head Department or his/her nominated deputy.

6. COMPLAINTS

6.1 Any complaints about the SIL CCTV system should be addressed to the Head HR-Department of SIL.

6.2 Complaints will be investigated in accordance with Section 5 of this policy.

Emergency Management of Information Technology

Policy Number: SIL-IT-EM-0001

Policy Date: 1ST May 2023

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the business.

Procedures

IT Hardware Failure

Where there is failure of any of the business's hardware, this must be referred to IT Department immediately.

It is the responsibility of concern Department to take relevant actions that should be undertaken with relevant AMC provider in the event of IT hardware failure.

It is the responsibility of IT Department to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to SIL operations.

Point of Sale Disruptions

In the event that point of sale (POS) system is disrupted, the following actions must be immediately undertaken:

- POS provider to be notified
- Concern Department must be notified immediately
- All POS transactions to be taken using the manual machine located below the counter
- For all manual POS transactions, customer signatures must be verified

Virus or other security breach

In the event that the SIL information technology is compromised by software virus or other relevant possible security breaches such breaches are to be reported to IT Department immediately.

IT department is responsible for ensuring that any security breach is dealt with within minimum timeframe to minimise disruption to business operations.

Signed: Harmander Singh Sidhu.

Position: General Manager-IT

Date: 01-July-2023.