Sparkline complete solution for material handling

Services By Trida Engineering Services

Information Technology

Policy and Procedure Manual

Table of Contents

Introduction 2

Technology Hardware Purchasing Policy 3

- Purpose of the Policy 3
- Procedures 3

Policy for Getting Software 7

- Purpose of the Policy 7
- Procedures 7

Policy for Use of Software 9

- Purpose of the Policy 9
- Procedures 9

Bring Your Own Device Policy 11

- Purpose of the Policy 11
- Procedures 11

Information Technology Security Policy 14

- Purpose of the Policy 14
- Procedures 14

Information Technology Administration Policy 16

- Purpose of the Policy 16
- Procedures 16

Website Policy 17

- Purpose of the Policy 17
- Procedures 17

Emergency Management of Information Technology 18

- Purpose of the Policy 18
- Procedures 18

Introduction

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

Sparkline Equipments Pvt. Ltd .will keeps 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: SEPL/IT/HW/PUR01

Policy Date: 10/06/2017

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

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

The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

Purchasing desktop computer systems

The desktop computer systems purchased must run a Windows XP, Windows7, Windows 8, Windows 10, and Linux and integrate with existing hardware the business server.

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

The desktop computer system bundle must include:

Desktop tower

Desktop screen of 17”, 22”.

- Keyboard and mouse You may like to consider stating if these are to be wireless

- Windows XP, Windows7, Windows 8, Windows 10 ,Linux, and software Office 2007/13/16
- speakers, microphone, webcam, printers etc.

The minimum capacity of the desktop must be:

- processor 1.5 GHz to 2.5 Ghz
- RAM 2 Gb to 8 Gb
- USB Port 2 to 8

Any change from the above requirements must be authorised by IT Department

All purchases of new desktops must be supported by guarantee and/or warranty requirements As per OEM

All purchases for desktops must be in line with the purchasing policy in the Purchase Process & Commercial Rules.

Purchasing portable computer systems (LAPTOPS).

The purchase of portable computer systems includes notebooks, laptops, tablets etc.}

Portable computer systems purchased must run a Windows XP, Windows7, Windows 8, Windows 10 ,Linux and integrate business server

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

The minimum capacity of the portable computer system must be:

- 2.3 GHz
- RAM 4GB to 8GB
- USB ports 1 x 3.0 , 2 x2.0
- DVD drive Mouse etc

The portable computer system must include the following software provided:

- Office 2007/2013, Adobe, Reader, Internet Explorer ,Mozilla firebox, team viewer,

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

All purchases for desktops must be in line with the purchasing policy in the Purchase Process & Commercial Rules.

Laptop Handover document

Mr. / Ms --

Working At ---

Specification:- ---

Signature:

Date:

Issuing Authority

- The laptop has been issued to the said individual with the below mentioned Understanding.
- Laptop issued is for solely official purpose.
- The employee shall be fully accountable for theft, loss or damage of the property.
- Employee can mention necessary specification needed for their job function before taking handover from the system admin department.
- Any additional software/hardware required by employee (before or after taking the handover) should be clearly communicated though mail to system admin department.
- Management is at the sole discretion on approving such request.
- In case of any malfunction, employees are required to report the same to the system Admin Department.
- Employee may not take the laptop for repair to any external agency /vendor at any point of time.
- The laptop should be return to the system admin department in case of leaving the organization or if they do not intend to use it for any reason.
- The employee shall be liable to replace or pay an equivalent amount to the organization in case of theft, loss or damage to the property .the organization retains the right to deduct the same from salary in case of such an event.

I--- , have read and understood the terms and condition said

by ---and declare to abide by them.

Signature: **Date :**

Employee Name:

Remark:-

Purchasing server systems

Server systems can only be purchased by IT Head, recommended IT Engineer.

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

All purchases of server systems must be supported by business are other server systems.

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

All purchases for server systems must be in line with the purchasing policy in the Purchase Process & Commercial Rules.

Purchasing computer peripherals

Computer system peripherals include 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.

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 IT Head, recommended IT Engineers.

All purchases of computer peripherals must be supported by guarantee and/or warranty requirements 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 Purchase Process & Commercial Rule.

Policy for Getting Software

Policy Number: SEPL/IT/SW/PUR01

Policy Date: 10/06/2017.

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 non-commercial software such as open source, freeware, etc. must be approved by respected dept. head 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 IT Head.

All purchased software must be purchased from relevant suppliers.

All purchases of software must be supported by guarantee and/or warranty requirements and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by IT Head

All purchases for software must be in line with the purchasing policy in the Purchase Process & Commercial Rule

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 respected HOD 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.

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

Policy for Use of Software

Policy Number: SEPL/IT/SW/USE01

Policy Date: 10/06/2017.

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 Head to ensure these terms are followed.

IT Head 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.

Sparkline Equipments Pvt. Ltd.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 Engineer.

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 responsibility of Respective HOD

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

Unless express approval from Respective HOD 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 Respected HOD 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 business and must be recorded on the software register by IT Engineer.

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 Respective HOD for consequence here, such as further consultation, reprimand action etc.The illegal duplication of software or other copyrighted works is not condoned within this business and Respective HOD 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 Respective HOD for consequence here, such as further consultation, reprimand action etc.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify Respective HOD 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 Respected HOD for consequence here, such as further consultation, reprimand action etc.

Bring Your Own Device Policy

Policy Number: SEPL/IT/ODO01

Policy Date: 10/06/2017

At Sparkline Equipments Pvt. Ltd. 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 Sparkline Equipments Pvt. Ltd.'s 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 Laptops for business purposes. All staff who use or access Sparkline Equipments Pvt. Ltd.'s 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:

- Notebooks, Laptops, smart phones, tablets, iPhone, removable media etc.

Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with IT Engineer.

IT Engineer will record the device and all applications used by the device.

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

- Email access, business internet access, business telephone calls etc.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes intellectual property, other employee details etc.

- Not to use the registered mobile device as the sole repository for Sparkline's information. All business information stored on mobile devices should be backed up

- To make every reasonable effort to ensure that Sparkline's 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 with current operating software, current security software etc. Not to share the device with other individuals to protect the business data access through the device

- To abide by Sparkline's internet policy for appropriate use and access of internet sites etc.

- To notify Sparkline's 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 Sparkline's 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 grants an exemption. Any requests for exemptions from any of these directives should be referred to the IT department.

Breach of this policy

Any breach of this policy will be referred to IT Dept.who will review the breach and determine adequate consequences, which can include insert consequences here such as confiscation of the device and or termination of employment.

Indemnity

Sparkline Equipments Pvt. Ltd. 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 indemnifies Sparkline Equipments Pvt. Ltd. against any and all damages, costs and expenses suffered by Sparkline Equipments Pvt. Ltd. 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 Sparkline Equipments Pvt. Ltd..

Additional Policies for Business Mobile Phone Use

Technology Hardware Purchasing Policy

Use of Software policy

Purchasing Policy

Information Technology Security Policy

Policy Number: SEPL/IT/SEC01

Policy Date: 10/06/2017

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, lock etc. It will be the responsibility of IT Engineer 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 Head 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 laptop, notepads, iPads, mobile phones etc.Each employee is required to use locks, passwords, etc.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 IT Head will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All laptop, notepads, iPads etc.when kept at the office desk is to be secured by relevant security measure here, such as keypad, lock etc.provided by IT Engineer Information Security

All 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 Engineer to ensure that data back-ups are conducted Daily frequency of back-ups here and the backed up data is kept in Back up Server & offsite venue.

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

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements.

Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to set a password for access As per his requirement.

Each password is to be rules relating to password creation here, such as number of alpha and numeric etc.and is not to be shared with any employee within the business.

IT Engineer 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 Five attempts then{insert relevant job title here}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
ERP	IT Engineer
Mobile	IT Engineer
Mail Server	IT Engineer

Employees are not authorised to use business computers for personal use such as internet usage etc.

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

Additional Policies for Information Technology Security

Information Technology Administration Policy

Information Technology Administration Policy

Policy Number: SEPL/IT/ADM001

Policy Date: 10/06/2017

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 IT engineer's System. It is the responsibility of IT Engineer 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 Engineer 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 Engineer is responsible for maintaining adequate technology spare parts and other requirements such as toners, printing paper etc.

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

Any unspecified technology administration requirements should be directed to IT Head Additional Policies for Information Technology Administration

Website Policy

Policy Number: SEPL/IT/WEB001

Policy Date: 10/06/2017

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 Engineer.

IT Head 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 Sales person All content on the website must follow relevant business requirements here where applicable, such as a business or content plan etc.

The content of the website is to be reviewed monthly.

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

Business Development dept. Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.

Emergency Management of Information Technology

Policy Number: SEPL/IT/EMG001

Policy Date: 10/06/2017

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 Engineer immediately.

It is the responsibility of IT Engineer to relevant actions that should be undertaken in the event of IT hardware failure.

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

Virus or other security breach

In the event that the business's information technology is compromised by software such breaches are to be reported to IT Engineer immediately.

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

Approved BY

Managing Director **Date.30/06/2017**