Introduction

The Sea Soft 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 Sea Soft will use to administer these policies, with the correct procedure to follow.

Sea Soft 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: 123.54.66

Policy Date: 11/2/2024

Guidance: This policy should be read and carried out by all staff. Edit this policy so it suits the needs of your business.

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

Guidance: The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy. Edit this statement to cover the relevant technology for your business.

Purchasing desktop computer systems

Guidance: For assistance with Choosing hardware and software, including desktop computers, the Business Victoria's Choosing hardware and software page on the Business Victoria website.

The desktop computer systems purchased must run a {insert relevant operating system here e.g. Windows} and integrate with existing hardware.

The desktop computer systems must be purchased as standard desktop system bundle and must be from HP or Dell.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of 24-inch.

- Keyboard and mouse You may like to consider stating if these are to be wireless
- Windows 11
- Printers and Speakers

The minimum capacity of the desktop must be:

- 3.6 GHz
- 16 GB of RAM
- 3 USB ports

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

All purchases of desktops must be compatible with the business's 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 laptop or notebooks.

Portable computer systems purchased must run a Windows and integrate with existing hardware.

The portable computer systems purchased must be HP or Dell.

The minimum capacity of the portable computer system must be:

- 2.4 GHz
- 8 GB of RAM
- 1 or 2 USB ports

The portable computer system must include the following software provided:

- Office 2013
- Adobe, Reader
- Internet Explorer

All purchases of desktops must be compatible with the business's 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 server engineer.

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

All purchases of server systems must be supported by {insert guarantee and/or warranty requirements here} and be compatible with the business's other server systems.

Any change from the above requirements must be authorised by server engineer.

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 printers, scanners, external hard drives.

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.

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

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 Samsung to ensure the business takes advantage of volume pricing-based discounts provided by Samsung. 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 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 Manager prior to purchase.

Any change from the above requirements must be authorised by Manager

All purchases of all mobile phones must be supported by guarantee and/or warranty

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

Additional Policies for Purchasing Hardware

Guidance: add, link or remove the policies listed below as required.

Purchasing Policy

Mobile phone policy

Policy for Getting Software

Policy Number: 123.54.76

Policy Date: 11/2/2024

Guidance: This policy should be read and carried out by all staff. Edit this policy so it suits the needs of your business.

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 must be approved by software engineer 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 software engineer

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

Any changes from the above requirements must be authorised by software engineer

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 software engineer 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 software engineer

Additional Policies for Obtaining Software

Guidance: add, link or remove the policies listed below as required.

Purchasing Policy

Use of Software policy

Policy for Use of Software

Policy Number: 123.54.87

Policy Date: 11/2/2024

Guidance: This policy should be read and carried out by all staff. Edit this policy so it suits the needs of your business.

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 software engineer to ensure these terms are followed.

Software engineer 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.

Sea Soft 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 {insert relevant job title here}

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 software engineer.

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

Unless express approval from software engineer 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 software engineer 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 software 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 the IT Manager for disciplinary action, up to and including termination of employment. The illegal duplication of software or other copyrighted works is not condoned within this business and the IT Manager 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 **the IT Manager** for **formal review and disciplinary action**, which may include a written warning, suspension of system access, or termination depending on the severity of the breach.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify **the IT Manager** 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 **the Operations Manager** for **further consultation and potential disciplinary measures** in line with Sea Soft's Code of Conduct.

Additional Policies for Use of Software

Guidance: add, link or remove the policies listed below as required.

Technology Hardware Policy

Obtaining Software policy

Bring Your Own Device Policy

Policy Number: 123.54.42

Policy Date: 11/2/2024

Guidance: Edit this policy so it suits the needs of your business.

At Sea Softwe 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 company'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, smartphones, tablets, and wearable devices such as smartwatches or portable storage drives for business purposes. All staff who use or access Sea Soft'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 and laptops running Windows 10 or higher
- Smartphones, including Android and iPhone devices
- Tablets such as iPad or Android-based tablets
- Removable media devices such as encrypted USB drives and external hard drives

Registration of personal mobile devices for business use

Guidance: You will need to consider if the business is to have any control over the applications that are used for business purposes and/or used on the personal devices.

Employees using personal devices for business purposes must register the device with **the IT Department under the supervision of the IT Manager**.

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, source code, client data, employee personal details, financial records, and confidential project plans**.
- Not to use the registered mobile device as the sole repository for company 's information. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that company'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
- Not to share the device with other individuals to protect the business data access through the device
- To notify Sea Softimmediately in the event of loss or theft of the registered device

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 the IT Security Manager grants an exemption. Any requests for exemptions from any of these directives should be referred to the IT Security Department.

Breach of this policy

Any breach of this policy will be referred to the Chief Information Security Officer (CISO) who will review the breach and determine adequate consequences, which can include confiscation of the device, suspension of access to company systems, formal disciplinary action, and/or termination of employment.

Indemnity

Sea Softbears 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 Sea Softagainst any and all damages, costs and expenses suffered by Sea Softarising 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.

Additional Policies for Business Mobile Phone Use

Guidance: add, link or remove the policies listed below as required.

Technology Hardware Purchasing Policy

Use of Software policy

Purchasing Policy

Information Technology Security Policy

Policy Number: 123.54.67

Policy Date: 11/2/2014

Guidance: This policy should be read and carried out by all staff. Edit this policy so it suits the needs of your business.

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 **keycard entry systems, biometric scanners, or secure locks**.

It will be the responsibility of **the IT Infrastructure Manager** 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 **the IT Infrastructure Manager** immediately.

All security and safety of all portable technology, **laptops, tablets, smartphones, and external storage devices** will be the responsibility of the employee who has been issued with the **laptop, tablet, smartphone, or external storage device**. Each employee is required to use **passwords, device encryption, and physical locks** 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 IT Security Manager** will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All **laptops, tablets, and smartphones** when kept at the office desk are to be secured by **cable locks or secure docking stations** provided by **the IT Department**.

Information Security

All **sensitive business data, client information, financial records, project files, and source code** is to be backed up.

It is the responsibility of **the IT Backup Administrator** to ensure that data back-ups are conducted **daily** and the backed-up data is kept **securely in the cloud and at an offsite storage facility**

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

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 every **90 days**.
Each password is to be **a minimum of 12 characters, containing at least one uppercase letter, one lowercase letter, one number, and one special character**, and is not to be shared with any employee within the business.
The IT Security Administrator 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 **the IT Security Administrator** 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.

Employees are only authorised to use business computers for personal use {insert 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.

Additional Policies for Information Technology Security

Guidance: add, link or remove the policies listed below as required.

Emergency Management of Information Technology Policy

Information Technology Administration Policy