SAMPLE INFORMATION TECHNOLOGY MANUAL

JULY 2019

Disclaimer

The information in this publication is for general guidance to ICPAU Accounting Firms. ICPAU does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. ICPAU, its employees and agents do not accept any liability to any person for the information or advice given in this document.

TABLE OF CONTENTS

Introduction

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

ABC & Company 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.

Approved on: _____

Approved by: _____

Signature: _____

Technology Hardware Purchasing Policy

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.

Purchasing desktop computer systems

The desktop computer systems purchased must run the latest version of Operating System and be able to integrate with existing hardware.

The desktop computer systems must be purchased as standard desktop system bundle and must be within the firm's approved manufacturer type.

All purchases of desktops must be supported by guarantee and warranty and be compatible with the firm's server system.

All purchases for desktops must be in line with the firm's purchasing policy.

Purchasing portable computer systems

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

Portable computer systems purchased must be able to integrate with existing hardware including the firm's servers.

The portable computer systems purchased must be within the firm's approved manufacturer type

All purchases of all portable computer systems must be supported by guarantee and warranty and be compatible with the firm's server system.

All purchases for portable computer systems must be in line with the firm's purchasing policy.

Purchasing server systems

Server systems can only be purchased by the firm's IT specialist.

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

All purchases of server systems must be supported by guarantee and warranty requirements and be compatible with the firm's other server systems.

All purchases for server systems must be in line with the firm's purchasing.

Purchasing computer peripherals

Computer system peripherals add-on devices such as printers, scanners, external hard drives etc 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 firm's other hardware and software systems.

All purchases for computer peripherals must be in line with the firm's purchasing policy.

Purchasing mobile telephones

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

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

The mobile phone purchased must be from the firm's approved supplier.

The request for accessories must be included as part of the initial request for a phone.

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 firm's purchasing policy.

Policy for Getting Software

Guidance: This policy should be read and carried out by all staff.

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 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 from reputable software sellers.

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

All purchases for software must be in line with the firm's purchasing policy.

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 must be obtained prior to the download or use of such software.

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

Policy for Use of Software

Guidance: This policy should be read and carried out by all staff.

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 allsoftware 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 each staff to ensure these terms are followed.

The firm's IT Specialist 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.

ABC & Company 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 firm's computers.

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 firm.

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.

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

Unless express approval from Managing Partber is obtained, software cannot be taken home and loaded on an 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 should be obtained 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 the firm's IT Specialist.

Unauthorised software is prohibited from being used in the firm. 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. The illegal duplication of software or other copyrighted works is not condoned within this firm and the firm 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 for disciplinary action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Managing Partner 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 for appropriate reprimand action.

Bring Your Own Device Policy

At ABC & Company 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 ABC & 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, smart phones, tablets and any other portable devices for business purposes. All staff who use or access ABC & Company's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with the firm's IT Specialist who 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 business or personal information that the firm considers sensitive to the business, for example intellectual property, other employee details etc.

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

- To make every reasonable effort to ensure that ABC & 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.

- To maintain and ensure that the device is up-to-date with the 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 ABC & Company's internet policy for appropriate use and access of internet sites etc.

- To notify ABC & Company 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 ABC & Company's equipment.

All employees who have a registered personal mobile device for business use acknowledge that ABC & Company:

- 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 Managing Partner grants an exemption.

Breach of this policy

Any breach of this policy will be referred to Managing Partner who will review the breach and determine adequate consequences, which can include confiscation of the device and/or disciplinary action.

Indemnity

ABC & Company bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using the firm's resources or facilities. All staff indemnifyABC & Company against any and all damages, costs and expenses suffered by ABC & Company 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 this policy may result independently from any action by ABC & Company.

Information Technology Security Policy

Guidance: This policy should be read and carried out by all staff.

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 and/or lock.

It will be the responsibility of the IT Specialist 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 Managing Partner immediately.

All security and safety of all portable technology including laptops, notepads, iPads and mobile phones will be the responsibility of the employee who has been issued with the device. Each employee is required to use locks and 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 IT Specialist will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All portable devices when kept at the office desk are to be secured by keypad or lock provided by the firm.

Information Security

All relevant data (including sensitive, valuable, or critical business data) on firm devices shall be backed up.

It is the responsibility of each employee to ensure that regular data back-ups are conducted and the backed up data is kept on the cloud, offsite venue, or any other designated place.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the IT Specialist 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 firm's confidentiality requirements. Any employee breaching this will be subjected to disciplinary action.

Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to reset his or her password for access every month.

Each password is to be of sufficient strength/complexity and is not to be shared with any employee within the business.

The firm's IT Specialist 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 Specialist 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 when this is allowable and for restricted purposes.

For internet and social media usage, refer to the internet and social media usage policy.

Guidance: This policy should be read and carried out by all staff.

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. It is the responsibility of the firm's IT Specialist to ensure that this register is maintained and up-to-date. 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.

The firm's IT Specialist is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by the Managing Partner.

The firm's IT Specialist is responsible for maintaining adequate technology spare parts and other requirements including toners, cartridges etc.

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

Any unspecified technology administration requirements should be directed to the Managing Partner.

Guidance: This policy should be read and carried out by all staff.

Purpose of the Policy

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

Procedures

Website Register

The website register must record the following details:

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

The firm's IT Specialist shall be responsible for keeping of the website register up to date and 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.

The content of the website is to be reviewed monthly.

The Managing Partner shall appoint persons are authorised to make changes to the firm's website.

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

All data collected from the website is to adhere to the Data Protection and Privacy Act, 2019.

Electronic Transactions Policy

Guidance: This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the business.

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

Electronic Funds Transfer (EFT)

It is the policy of ABC & Company that all payments and receipts should be made by EFT where appropriate.

All EFT payments and receipts must adhere to the firm's finance manual.

All EFT arrangements, including receipts and payments must be submitted to finance department.

EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy.

EFT payments must be appropriately recorded in line with Finance Manual.

EFT payments once authorised shall be recorded.

EFT payments can only be released for payment once pending payments have been authorised by the Managing Partner.

For good control over EFT payments, the persons authorising the payments and making the payment shall not be the same person.

All EFT receipts must be reconciled to customer records once a week.

Where EFT receipt cannot be allocated to customer account, it is responsibility of Head of Finance Department to investigate. In the event that the customer account cannot be identified within one month the receipted funds must be allocated to suspense account or returned to source etc and the Managing Partner must authorise this transaction.

The Managing Partner shall annually review EFT authorisations for initial entry, alterations, or deletion of EFT records, including supplier payment records and customer receipt records.

Electronic Purchases

All electronic purchases by any authorised employee must adhere to the purchasing policy in the Finance Manual.

Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken using business credit cards only and therefore adhere to the business credit card policy in the Finance Manual.

IT Service Agreements Policy

This policy should be read and carried out by all staff.

Purpose of the Policy

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

Procedures

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

- 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 must be reviewed by the Managing Partner and/or the firm's lawyer before the agreement is entered into.

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

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 IT Specialist.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, the Managing Partner and/or the firm's lawyer shall review before the renewal is entered into.

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 Managing Partner and/or the firm's lawyer for the settlement of such dispute.

Emergency Management of Information Technology

This policy should be read and carried out by all staff.

Purpose of the Policy

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

Procedures

IT Hardware Failure

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

It is the responsibility of every staff to ensure that relevant actions are undertaken in the event of IT hardware failure.

It is the responsibility of the firm's IT Specialist 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 firm's information technology is compromised by software virus or other relevant possible security breaches such breaches are to be reported to the firm's IT Specialist immediately.

The firm's IT Specialist is responsible for ensuring that any security breach is dealt with within the appropriate timeframe to minimise disruption to business operations.

Website Disruption

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- Managing Partner must be notified immediately.