Consortium For Training Research a Development (CTRD)

IT Policy

Table of Contents

Introduction-:

- CTRD's IT Policy and Procedure 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 CTRD will use to administer these policies, with the correct procedure to follow.

- CTRD 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: **CTRD/1023/12**

Policy Date: {10.1.2015}

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

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

- 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 Windows 10 and integrate with existing hardware.
- 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 14"

- Keyboard and mouse.

- Windows 7, and software Office 2010
- Speakers, printers etc.

The minimum capacity of the desktop must be:

- Processor –dual core- 2.4 GHz + (i5 or i7 Intel processor or equivalent AMD)
- RAM-16 GB
- 3 of USB ports
- Monitor 19” LCD, 14” Desktop
- Backup Device- External Hard Drive(256 GB)-3 , Pen drives- 3
- Any change from the above requirements must be authorised by Secretary/President.
- All purchases of desktops must be supported by warranty of minimum 4 years and have to be compatible with the organisation’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 must includes such as notebooks, laptops, tablets etc.

The minimum capacity of the portable computer system must be:

- Processor-dual core @2.4 GHz (i5 and i7 Intel processor or equivalent AMD)
- RAM-8 GB
- 4 number of USB ports here}
- DVD drive, microphone port, webcam, speakers

The portable computer system must include the following software provided:

- Office Package 2010, Adobe Reader, Internet Explorer, PDF maker and converter
- Antivirus
- Network sharing
- Any change from the above requirements must be authorised by Secretary/ President.
- All purchases of all portable computer systems must be supported by 2 years or equivalent warranty.
- All purchases for portable computer systems must be in line with the purchasing policy in the financial policies and procedures.

Purchasing server systems

- Server systems can only be purchased is subject to approval from Secretary /President of the Organization and also recommended by 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 and be compatible with the CTRD's other server systems.
- Any change from the above requirements must be authorised by Secretary/ President of CTRD.
- All purchases for server systems must be in line with the purchasing policy in the financial policies and procedures.

Purchasing computer peripherals

- Computer system peripherals include add-on devices such as printers, scanners, external hard drives etc.
- Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.
- 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 Secretary/ President.
- All purchases of computer peripherals must be supported by 4 years warranty requirements and be compatible with the organization's other hardware and software systems.
- Any change from the above requirements must be authorised by Secretary/President.
- All purchases for computer peripherals must be in line with the purchasing policy in the financial policies and procedures.

Purchasing mobile telephones

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

- The mobile phone must be compatible with the business's current hardware and software systems.
- The mobile phone purchased should be from renowned company and must have warranty.

- 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 Secretary/ President of the organization prior to purchase.
- Any change from the above requirements must be authorised by Secretary/ President of the CTRD.
- All purchases for mobile phones must be in line with the purchasing policy in the financial policies and procedures.

Policy for Getting Software

Policy Number: **CTRD/1023/12**

Policy Date: {10.1.2015}

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, you tube, converter etc. Here must be approved by Secretary/ President of the Organization 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 Admin
- All purchased software must be purchased from authentic vendor
- All purchases of software must be supported by guarantee and/or warranty of 2-3 years and be compatible with the business's server and/or hardware system.
- Any changes from the above requirements must be authorised by Secretary/President.
- All purchases for software must be in line with the purchasing policy in the financial policies and procedures manual.

Policy for Use of Software

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 5 Desktops and one laptop, then it is the responsibility of admin to ensure these terms are followed.
- IT department is responsible for completing a software audit of all hardware once 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.

- Consortium for Training Research and Development 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 responsibility of Admin.
- Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.
- Unless express approval from Secretary/ President 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 Secretary/ President 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 Admin.
- 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 punishable.

Breach of Policy

- Where there is a breach of this policy by an employee, that employee will be referred to answerable to the authority of the organization and 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 by the admin immediately.

Information Technology Security Policy

Policy Number: **CTRD/1023/12**

Policy Date: {10.1.2015}

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
- It will be the responsibility of Admin 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 Secretary/ President 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. Each employee is required to use 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 department and Admin will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

Information Security

- All relevant data should be backed up – either general such as sensitive, valuable, or critical business data is to be backed-up.
- It is the responsibility of IT Department and Admin to ensure that data back-ups are conducted and the backed up data is kept safely.
- All technology that has internet access must have anti-virus software installed. It is the responsibility of user of the device is 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.

Information Technology Administration Policy

Policy Number: **CTRD/1023/12**

Policy Date: {10.1.2015}
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 on the register. It is the responsibility of Admin 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.
- Admin is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by Secretary /President. Admin is responsible for maintaining adequate technology spare parts and other requirements including toners, printing paper etc.
- A technology audit is to be conducted annually by IT Department to ensure that all information technology policies are being adhered to.

Website Policy

Policy Number: **CTRD/1023/12**

Policy Date: {10.1.2015}

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.
- It Department 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 IT Department
- All content on the website must follow relevant business requirements where applicable, such as a business or content plan etc.
- The content of the website is to be reviewed quarterly.
- The following persons are authorised to make changes to the business website:- IT Department
- 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 Privacy Act.

Electronic Transactions Policy

Policy Number: **CTRD/1023/12**

Policy Date: {10.1.2015}

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 Consortium for Training Research and Development that all payments and receipts should be made by EFT where appropriate.

- All EFT payments and receipts must adhere to all finance policies in the financial policies and procedures manual.
- All EFT arrangements, including receipts and payments must be submitted to accounts 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 policy.
- EFT payments can only be released for payment once pending payments have been authorised by Secretary/ President.
- For good control over EFT payments, ensure that the persons authorising the payments and making the payment are not the same person.
- All EFT receipts must be reconciled to customer records daily basis.
- It is the responsibility of Accounts Department to 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 financial policies and procedures 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.

IT Service Agreements Policy

This policy should be read and carried out by all staff. Addition /Alteration of this policy are subject to the need of the organization.

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 recommended lawyer or solicitor before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Secretary/ President.
- All IT service agreements, obligations and renewals must be recorded
- 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 Secretary/ President.

Emergency Management of Information Technology

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 Section immediately. It is the responsibility of IT Department to should be undertaken here in the event of IT hardware failure. It is their responsibility of to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to business 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
- IT 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 business's information technology is compromised by software virus or such breaches are to be reported to Secretary/ President immediately.
- It section of the CTRD office is responsible for ensuring that any security breach is dealt with within 3 days 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
- It Department must be notified immediately
- Take proper action within next 12 hours.