Information Technology Policy and Procedure Manual Template

From https://www.business.vic.gov.au/

Note: Delete this and the next page once you complete the template.

Who should use this template?

Small to medium sized business owners who use information technology in their business.

Why use a policy and procedure manual?

This Information Technology (IT) policy and procedure manual is for the small to medium sized business owner and their employees.

The main benefits to having this policy and procedure manual:

- ensures all staff are aware of obligations in relation to selection, use and safety when utilising information technology within the business
- is a proven way to help your managers and supervisors make consistent and reliable decisions
- helps give each employee a clear understanding as to what you expect and allow.

It takes a little effort to complete, but brings definite long-term benefits, reduces disputes, and adds to the professionalism of your business.

How to complete this template

Designed to be customised

This template for an IT policy and procedures manual is made up of example topics. You can customise these if you wish, for example, by adding or removing topics.

To complete the template:

1. Guidance text appears throughout the document, marked by the word Guidance. Where you see a guidance note, read and then delete it. Guidance has been added to help you complete the template and should not appear in your final version.

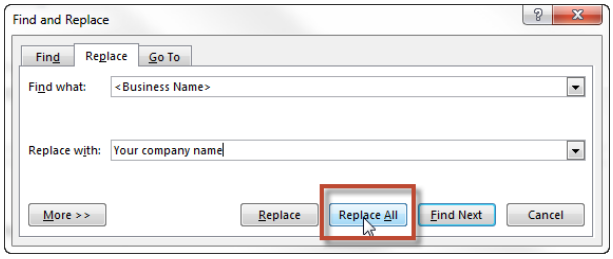
2. Using Word's Replace function, search for {Business Name} and replace with your company name.

    a) In Word's Home ribbon, open the Find and Replace tool, choose Replace to open the Find and Replace tool. The Find and Replace dialog opens with the Replace tab selected.

    b) Enter {Business Name} in the Find what field.

    c) Enter your company name in the Replace with field.

    d) Click Replace All



3. Replace {items in curly brackets} with your own wording.

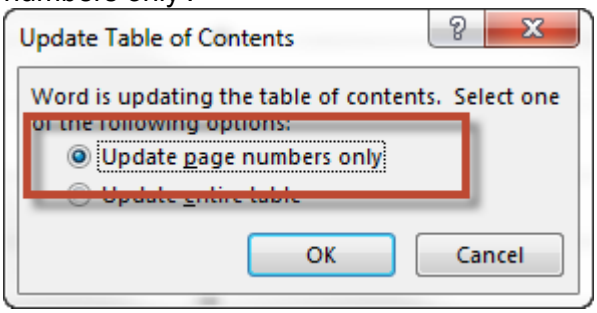
4. Where you see a reference to other policies, insert a link to another example policy that applies in your business

5. Once you have finished work on the template, delete the first three pages of the document.

6. Lastly refresh the page numbers in the table of contents.

    a. Right mouse click on the table of contents

b. In the small menu that appears, choose ‘Update Field’ then ‘Update page numbers only’.



Other tips

- To stop this policy manual sitting on a desk collecting dust, make it a living document. How? Ask your staff for their thoughts on how to improve it. Then review it every six months.
- Make explaining your policies and procedures an important part of your induction process.
- Leave the words ‘Document valid when printed only’ in the footer to remind the reader they might be using an out-of-date copy. (The ‘Last printed’ date automatically updates in the footer when you print. You don’t need to update this.) Try to destroy or archive all out-of-date copies.
- The writing style doesn’t need to be formal or longwinded to be effective. Use simple sentences and plain English to reduce the chance an employee or manager will be confused about the intent of your policy or the way to carry out a procedure.

Note: Delete this and the previous page once you complete the template.

Disclaimer

{Insert Company Logo Here}

Information Technology
Policy and Procedure Manual

Table of Contents

Information Technology Policy and Procedure Manual 1
Introduction 3
Technology Hardware Purchasing Policy 4
Purpose of the Policy 4
Procedures 4
Policy for Getting Software 9
Purpose of the Policy 9
Procedures 9
Policy for Use of Software 11
Purpose of the Policy 11
Procedures 11
Bring Your Own Device Policy 14
Purpose of the Policy 14
Procedures 14
Information Technology Security Policy 18
Purpose of the Policy 18
Procedures 18
Information Technology Administration Policy 21
Purpose of the Policy 21
Procedures 21
Website Policy 23
Purpose of the Policy 23
Procedures 23
Electronic Transactions Policy 25
Purpose of the Policy 25
Procedures 25
IT Service Agreements Policy 27

Purpose of the Policy 27
Procedures 27
Emergency Management of Information Technology 29
Purpose of the Policy 29
Procedures 29

Introduction

The {Business Name} 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 {Business name} will use to administer these policies, with the correct procedure to follow.

{Business Name} 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: {insert unique number}

Policy Date: {insert date of policy}

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 { insert names of existing technology such as the business server}.

The desktop computer systems must be purchased as standard desktop system bundle and must be {insert manufacturer type here, such as HP, Dell, Acer etc.}.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of {insert screen size here}

- Keyboard and mouse You may like to consider stating if these are to be wireless
- {insert name of operating system, e.g. Windows 7, and software e.g. Office 2013 here}
- {insert other items here, such as speakers, microphone, webcam, printers etc.}

The minimum capacity of the desktop must be:

- {insert speed of computer size (GHz -gigahertz)here}
- {insert memory (RAM) size here}
- {insert number of USB ports here}
- {insert other specifications for desktop here, such as DVD drive, microphone port, etc.}

Any change from the above requirements must be authorised by {insert relevant job title here}

All purchases of desktops must be supported by{insert guarantee and/or warranty requirements here} and 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 {insert names of portable devices here, such as notebooks, laptops, tablets etc.}

Portable computer systems purchased must run a {insert relevant operating system here e.g. Windows} and integrate with existing hardware { insert names of existing technology such as the business server}.

The portable computer systems purchased must be {insert manufacturer type here, such as HP, Dell, Acer, etc.}.

The minimum capacity of the portable computer system must be:

- {insert speed of computer size (GHz -gigahertz)here}
- {insert memory (RAM) size here}
- {insert number of USB ports here}

- {insert other specifications for portable device here, such as DVD drive, microphone port, webcam, speakers, etc.}

The portable computer system must include the following software provided:

- {insert names of software e.g. Office 2013, Adobe, Reader, Internet Explorer here}
- {insert names of software e.g. Office 2013, Adobe, Reader, Internet Explorer here}
- {insert names of software e.g. Office 2013, Adobe, Reader, Internet Explorer here}

Any change from the above requirements must be authorised by {insert relevant job title here}

All purchases of all portable computer systems must be supported by{insert guarantee and/or warranty requirements here} and 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 {insert relevant job title here, recommended 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 {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 {insert relevant job title here}

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 {insert names of add-on devices such as printers, scanners, external hard drives etc. here}

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 {insert relevant job title here, recommended IT specialist or department manager}.

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

Any change from the above requirements must be authorised by {insert relevant job title here}

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 {insert names authorised suppliers here, such as Telstra etc.} to ensure the business takes advantage of volume pricing based discounts provided by {insert names authorised suppliers here, such as Telstra etc.}. 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 {insert manufacturer type here, such as IPhone, Blackberry, Samsung, etc.}.

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 {insert relevant job title here} prior to purchase.

Any change from the above requirements must be authorised by {insert relevant job title here}

All purchases of all mobile phones must be supported by{insert guarantee and/or warranty requirements here}.

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: {insert unique number}

Policy Date: {insert date of policy}

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, 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 {insert relevant job title here}

All purchased software must be purchased from {insert relevant suppliers names or the words ‘reputable software sellers’ here}

All purchases of software must be supported by{insert guarantee and/or warranty requirements here} and be compatible with the business’s server and/or hardware system.

Any changes from the above requirements must be authorised by {insert relevant job title here}

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 {insert relevant job title here} 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 {insert relevant job title here}

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: {insert unique number}

Policy Date: {insert date of policy}

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 {insert relevant job title here} to ensure these terms are followed.

{insert relevant job title here} 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.

{Business Name} 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 {insert relevant job title here}

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

Unless express approval from {insert relevant job title here} 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 {insert relevant job title here} 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 {insert relevant job title here}

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 {insert relevant job title here} for {insert 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 {insert relevant job title here} 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 {insert relevant job title here} for {insert 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 {insert relevant job title here} 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 {insert relevant job title here} for {insert consequence here, such as further consultation, reprimand action etc.}

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: {insert unique number}

Policy Date: {insert date of policy}

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

At {Business Name} 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 {Business Name}'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 {insert other types of mobile devices} for business purposes. All staff who use or access {Business Name}'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:

- {insert type of approved mobile devices such as notebooks, smart phones, tablets, iPhone, removable media etc.}
- {insert type of approved mobile devices such as notebooks, smart phones, tablets, iPhone, removable media etc.}
- {insert type of approved mobile devices such as smart phones, tablets, iPhone etc.}
- {insert type of approved mobile devices such as notebooks, smart phones, tablets, iPhone, removable media etc.}.

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 when using personal devices for business use will register the device with {insert relevant job title or department here}.

{insert relevant job title or department here} will record the device and all applications used by the device.

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

- {insert each type of approved use such as email access, business internet access, business telephone calls etc.}
- {insert each type of approved use such as email access, business internet access, business telephone calls etc.}
- {insert each type of approved use such as 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 {insert types of business or personal information that you consider sensitive to the business, for example intellectual property, other employee details etc.}
- Not to use the registered mobile device as the sole repository for {Business Name}'s information. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that {Business Name}'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 {insert maintenance requirements of mobile devices such as 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 {Business Name}'s internet policy for appropriate use and access of internet sites etc.
- To notify {Business Name} 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 {Business Name}'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 {insert relevant job title or department here} grants an exemption. Any requests for exemptions from any of these directives, should be referred to the {insert relevant job title or department here}.

Breach of this policy

Any breach of this policy will be referred to {insert relevant job title} 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

{Business Name} 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 {Business Name} against any and all damages, costs and expenses suffered by {Business Name} 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 {Business Name}.

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: {insert unique number}

Policy Date: {insert date of policy}

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 {insert relevant security measure here, such as keypad, lock etc.}

It will be the responsibility of {insert relevant job title here} 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 {insert relevant job title here} immediately.

All security and safety of all portable technology, {insert relevant types here, such as laptop, notepads, iPad etc.} will be the responsibility of the employee who has been issued with the {insert relevant types here, such as laptop, notepads, iPads, mobile phones etc.}. Each employee is required to use {insert relevant types here, such as 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, {insert relevant job title here} will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All {insert relevant types here, such as laptop, notepads, iPads etc.} when kept at the office desk is to be secured by {insert relevant security measure here, such as keypad, lock etc.} provided by {insert relevant job title here}

Information Security

All {insert 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 {insert relevant job title here} to ensure that data back-ups are conducted {insert frequency of back-ups here} and the backed up data is kept {insert where back up data is to be kept e.g. cloud, offsite venue, employees home etc. here}

All technology that has internet access must have anti-virus software installed. It is the responsibility of {insert relevant job title here} 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. Any employee breaching this will be {insert relevant consequence here}

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 {insert frequency here}

Each password is to be {insert 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.

{insert relevant job title here} 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 {insert a number here e.g. three 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**
{insert name or type of technology here}	{insert authorised persons or job titles here}
{insert name or type of technology here}	{insert authorised persons or job titles here}

Technology – Hardware/ Software	Persons authorised for access
{insert name or type of technology here}	{insert authorised persons or job titles here}
{insert name or type of technology here}	{insert authorised persons or job titles here}

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.

It is the responsibility of {insert relevant job title here} to keep all procedures for this policy up to date.

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

Information Technology Administration Policy

Policy Number: {insert unique number}

Policy Date: {insert date of policy}

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 administration of information technology assets and resources within the business.

Procedures

All software installed and the licence information must be registered on the {insert where these records are to be kept}. It is the responsibility of {insert relevant job title here} 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.

{insert relevant job title here} is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by {insert relevant job title here}.

{insert relevant job title here} is responsible for maintaining adequate technology spare parts and other requirements including {insert specific technology requirements here, such as toners, printing paper etc.}

A technology audit is to be conducted {insert frequency here e.g. annually} by {insert relevant job title here} to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to {insert relevant job title here}

Additional Policies for Information Technology Administration

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

IT Service Agreements Policy

Purchasing Policy

Website Policy

Policy Number: {insert unique number}

Policy Date: {insert date of policy}

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 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

{insert any other records to be kept in relation to your business website here}.

The keeping the register up to date will be the responsibility of {insert relevant job title here}.

{insert relevant job title here} 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 {insert relevant job title here}

All content on the website must follow {insert relevant business requirements here where applicable, such as a business or content plan etc.}

The content of the website is to be reviewed {insert frequency here}

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

{insert relevant job title here}

{insert relevant job title here}

{insert relevant job title here}

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

Additional Policies for Website Policy

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

Information Technology Security Policy

Emergency Management of Information Technology policy

Electronic Transactions Policy

Policy Number: {insert unique number}

Policy Date: {insert date of policy}

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 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 {Business Name} 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 {insert relevant department of the business here, e.g. finance department}.

EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the Financial policies and procedures manual.

EFT payments must be appropriately recorded in line with finance policy in the Financial policies and procedures manual.

EFT payments once authorised, will be entered into the {insert title of payment system here e.g. NAB online system} by {insert relevant job title here}

EFT payments can only be released for payment once pending payments have been authorised by {insert relevant job title here}

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 {insert frequency here e.g. once a week etc.}

Where EFT receipt cannot be allocated to customer account, it is responsibility of {insert relevant job title here} to investigate. In the event that the customer account cannot be identified within {insert length of time here, such as one month} the receipted funds must be {insert action here such as allocated to suspense account or returned to source etc.}. {insert relevant job title here} must authorise this transaction.

It is the responsibility of {insert relevant job title here} 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.

All electronic purchases must be undertaken using business credit cards only and therefore adhere to the business credit card policy in the Financial policies and procedures manual.

Additional Policies for Electronic Transactions Policy

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

Information Technology Security Policy

Finance Policies

IT Service Agreements Policy

Policy Number: {insert unique number}

Policy Date: {insert date of policy}

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 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:

Guidance: Insert the acceptable IT services for your business – the following dot points will assist.

- 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.
- {insert type of IT service here}.

All IT service agreements must be reviewed by {insert who should review, 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 {insert relevant job title here}

All IT service agreements, obligations and renewals must be recorded {insert where the agreements are to be recorded here}

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 {insert relevant job title here}.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, {insert who should review, recommended lawyer or solicitor} before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by {insert relevant job title here}

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 {insert relevant job title here} who will be responsible for the settlement of such dispute.

Additional Policies for IT Services Policy

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

Technology Hardware Purchasing Policy

Emergency Management of Information Technology

Policy Number: {insert unique number}

Policy Date: {insert date of policy}

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 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 {insert relevant job title here} immediately.

It is the responsibility of {insert relevant job title here} to {insert relevant actions that should be undertaken here} in the event of IT hardware failure.

It is the responsibility of {insert relevant job title here} to undertake tests on planned emergency procedures {insert frequency here, recommended 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:

Guidance: Insert the actions required for your business – the following dot points will assist.

- POS provider to be notified
- {insert relevant job title here} 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
- {insert other relevant emergency actions here}
- {insert other relevant emergency actions here}.

Virus or other security breach

In the event that the business's information technology is compromised by software virus or {insert other relevant possible security breaches here} such breaches are to be reported to {insert relevant job title here} immediately.

{insert relevant job title here} is responsible for ensuring that any security breach is dealt with within {insert relevant timeframe here} to minimise disruption to business operations.

Website Disruption

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

Guidance: Insert the actions required for your business – the following dot points will assist.

- Website host to be notified
- {insert relevant job title here} must be notified immediately
- {insert other relevant emergency actions here}
- {insert other relevant emergency actions here}.