Information Technology

Policy and Procedure Manual

Table of Contents

Introduction

The Infoways Pty Ltd (Infoways) 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 Infoways will use to administer these policies, with the correct procedure to follow.

Infoways 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.

Policy for Getting Software

Policy Number: INF00127

Policy Date: 15 January 2019

Purpose of the Policy

This policy provides guidelines for the purchase of software for the business to ensure that all software used by the business is appropriate, value for money and where applicable integrates with other technology for the business. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

Request for Software

All software, including non-commercial software such as open source, freeware, etc must be approved by Brent Welch or the Team Leader 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 Kara Vallins or the Accounts Payable Team.

All purchased software must be purchased from reputable software sellers.

All purchases of software must be supported by insert 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 Brent Welch or the Team Leader.

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 Brent Welch 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 Brent Welch.

Additional Policies for Obtaining Software

Purchasing Policy

Use of Software policy

Policy for Use of Software

Policy Number: INF00128

Policy Date: 15 January 2019

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 the Chief Information Officer to ensure these terms are followed.

The Chief Information Officer 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.

Infoways 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 staff.

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 the company Training Manager.

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

Unless express approval from the Chief Information Officer 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 the Chief Information Officer 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 the Chief Information Officer.

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 Chief Information Officer for further consultation, or reprimand action as required. The illegal duplication of software or other copyrighted works is not condoned within this business and Chief Information Officer 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 Chief Information Officer for further consultation or, reprimand action as required.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Chief Information Officer, or his/her representative 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 Chief Information Officer for further consultation and, or reprimand action as required.

Additional Policies for Use of Software

Technology Hardware Policy

Obtaining Software policy

Information Technology Security Policy

Policy Number: INF00129

Policy Date: 18 January 2019

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through keypad, lock etc.

It will be the responsibility of the nominated security officer 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 nominated security officer immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc will be the responsibility of the employee who has been issued with the laptop, notepads, iPads, mobile phone etc. Each employee is required to use locks, passwords, etc and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the nominated security officer 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, notepads, iPads etc, when kept at the office desk is to be secured by keypad, lock etc provided by the nominated security officer.

Information Security

All relevant data – either general such as sensitive, valuable, or critical business data is to be backed-up.

It is the responsibility of Brent Welch to ensure that data back-ups are conducted daily and the backed up data is kept either in the cloud, or offsite venue such as Digital Pacific back-up server.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the nominated security officer 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 referred to the Chief Information Officer for further investigation.

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 month.

Each password is to be alpha and numeric and is not to be shared with any employee within the business.

The nominated security officer 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 Team Leader 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.

For internet and social media usage, refer to the Human Resources Manual.

It is the responsibility of the Chief Information Officer to keep all procedures for this policy up to date.

Additional Policies for Information Technology Security

Emergency Management of Information Technology Policy

Information Technology Administration Policy

Information Technology Administration Policy

Policy Number: INF00130

Policy Date: 15 January 2019

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 software register. It is the responsibility of Chief Information Officer 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.

The Chief Information Officer is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by Chief Information Officer.

The nominated IT service officer 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 the Chief Information Officer or his/her representative to ensure that all information technology policies are being adhered to.

Additional Policies for Information Technology Administration

IT Service Agreements Policy

Purchasing Policy

Website Policy

Policy Number: INF00131

Policy Date: 15 January 2019

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 the Chief Information Officer.

The Chief Financial Officer 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 the Chief Information Officer.

All content on the website must follow the business and content plan.

The content of the website is to be reviewed monthly.

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

The Chief Information Officer

The Web Coordinator

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

Information Technology Security Policy

Emergency Management of Information Technology policy

Electronic Transactions Policy

Policy Number: INF00132

Policy Date: 18 January 2019

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 Infoways 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 the Accounts Team.

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 Xero and the NAB online system by the Accounts Team.

EFT payments can only be released for payment once pending payments have been authorised by the Chief Financial Officer.

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.

Where EFT receipt cannot be allocated to customer account, it is responsibility of the Accounts Team Leader 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. The Chief Financial Officer must authorise this transaction.

It is the responsibility of the Chief Financial Officer 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

Information Technology Security Policy

Finance Policies

IT Service Agreements Policy

Policy Number: INF00133

Policy Date: 27 February 2019

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
- Provision of business software
- Provision of SMS and Email services
- Website design, maintenance etc.

All IT service agreements must be reviewed before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Leadership Team.

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 the Chief Information Officer.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, it should be reviewed by the Leadership Team before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Chief Information Officer.

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 the nominated Project Manager who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Policy Number: INF00134

Policy Date: 05 June 2019

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 the nominated maintenance officer immediately.

It is the responsibility of the staff member to refer the issue in the event of IT hardware failure.

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

Virus or other security breach

In the event that the business's information technology is compromised by software virus or other relevant possible security breaches, such breaches are to be reported to the Chief Information Officer immediately.

The Chief Information Officer is responsible for ensuring that any security breach is dealt with within 1 hour to minimise disruption to business operations.

The Chief Information Officer is responsible for ensuring that all effected clients are advised immediately by phone and/or email.

Website Disruption

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

- Website host to be notified

- The Chief Information Officer must be notified immediately