Information Technology Policy and Procedure

REED CONDOMINIUM MANAGEMENT SOLUTIONS

MAXIMIZING VALUE, MINIMIZING HASSLES

Introduction

The Reed Condominium Management Solutions 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 Reed Condominium Management Solutions will use to administer these policies, with the correct procedure to follow.
Reed Condominium Management Solutions 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

Purpose of the Policy

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

Procedures

Request for Software

All software, must be approved by Network Administrator 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 Network Administrator
All purchases of software must be compatible with the business's server and/or hardware system.
Any changes from the above requirements must be authorized by Network Administrator

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 Network Administrator 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 authorized by Network Administrator

Additional Policies for Obtaining Software

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 licenses 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 Network Administrator to ensure these terms are followed.

The Network Administrator is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.
Reed Condominium Management Solutions 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 Network Administrator.
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 Network Administrator.
Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.
Unless express approval from Network Administrator is obtained, software cannot be taken home and loaded on a employees' home computer.
Where an employee is required to use software at home, a company computer will be provided to the employee.
Unauthorized 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 unauthorized duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorized copies of software will be referred to President/CEO for disciplinary action, such as further consultation, reprimand action or termination of employment. The illegal duplication of software or other copyrighted works is not condoned within this business and President/CEO is authorized to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to the President/CEO for disciplinary action, such as further consultation, reprimand action or termination of employment . Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Network Administrator 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 President/CEO for disciplinary action, such as further consultation, reprimand action or termination of employment

Bring Your Own Device Policy

At Reed Condominium Management Solutions 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 been requested to provide their own mobile devices to connect to Reed Condominium Management Solutions' 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 {Reed Condominium Management Solutions}'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:

- iPhone, Samsung or Galaxy smartphones.
- Laptop or tablet

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile 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 Network Administrator grants an exemption. Any requests for exemptions from any of these directives, should be referred to the Network Administrator.

Breach of this policy

Any breach of this policy will be referred to the President/CEO who will review the breach and determine adequate consequences, which can include disciplinary action, such as further consultation, reprimand action or termination of employment.

Indemnity

Reed Condominium Management Solutions 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 Reed Condominium Management Solutions against any and all damages, costs and expenses suffered by Reed Condominium Management Solutions 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 Reed Condominium Management Solutions.

Information Technology Security Policy

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.

It will be the responsibility of Network Administrator 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 Network Administrator 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 phones etc. Each employee is required to use two factor authentication 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, the Network Administrator will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All laptop, notepads, iPads etc. when kept at the office desk is to be secured by keypad, or lock provided by Network Administrator.

Information Security

All relevant data is to be backed daily, such as sensitive, valuable, or critical business data.
It is the responsibility of Network Administrator to ensure that data back-ups are conducted daily and the backed up data is kept in secure cloud storage.
All technology that has internet access must have anti-virus software installed. It is the responsibility of Network Administrator 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 President/CEO for disciplinary action, such as further consultation, reprimand action or termination of employment.

Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to set a two-factor authentication for access.
Each password is to be 8 characters long, with upper case, lower case, numeric and symbol and is not to be shared with any employee within the business.
Network Administrator is responsible for the issuing of the identification code and initial password for all employees.
Where an employee forgets the password or is 'locked out' after three attempts, then Network Administrator is authorized 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 not authorized to use business computers for personal use.
Employees are not authorized to use business computers for social media usage.
It is the responsibility of Network Administrator to keep all procedures for this policy up to date.

Information Technology Administration Policy

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 license information must be registered on the Reed Condominium Management Solutions records and are to be kept. It is the responsibility of Network Administrator to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What license agreements are in place for each software package
- Renewal dates if applicable.

Network Administrator is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by Network Administrator.
Network Administrator is responsible for maintaining adequate technology spare parts and other requirements including toners, printing paper etc.
A technology audit is to be conducted every 6 months by Network Administrator to ensure that all information technology policies are being adhered to.
Any unspecified technology administration requirements should be directed to the President/CEO.

IT Service Agreements Policy

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 Network Administrator 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 President/CEO.
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 authorized by President/CEO.
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 Network Administrator 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 President/CEO.
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 Network Administrator who will be responsible for the settlement of such dispute.

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 Network Administrator immediately.
It is the responsibility of Network Administrator to recover all data from secure cloud storage in the event of IT hardware failure.
It is the responsibility of Network Administrator to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimize disruption to business operations.

Virus or other security breach

In the event that the business's information technology is compromised by software virus or network breach such breaches are to be reported to Network Administrator immediately.
Network Administrator is responsible for ensuring that any security breach is dealt with immediately to minimize disruption to business operations.