SKYSPIN
STUDIOS

SSC
SKYSPIN COMMUNICATION
(SMC-PRIVATE) LIMITED

Information Technology
Policy & Procedure Manual

Version 1.0

This document is valid for
Skyspin Studios
&
Skyspin Communication (SMC-Private) Limited

Dated: 05-11-2020

Created by:
Muhammad Mashhood
(Assistant Manager IT)

Table of Contents

This page left blank intentionally

Introduction

The Skyspin Studios 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 Skyspin Studios will use to administer these policies, with the correct procedure to follow.

Skyspin Studios 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 Code: SSITPL20-HW

Policy Date: 05-11-2020

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

Purchasing desktop computer systems

The desktop computer systems purchased must run Microsoft® Windows 7,8,10 or Linux (any distribution) and integrate with existing hardware networking switches, modems or any other NAS (Network Attached Storage) devices.

The desktop computer systems must be purchased as standard desktop system bundle and must be Dell, HP, Lenovo, Acer, Asus, MSI, or any equivalent custom desktop.

The desktop computer system bundle must include:

Desktop tower

Desktop screen will be depended on the nature of the work a user will be doing.

- Keyboard and mouse, they could be wired or wireless of known brands.
- Microsoft® Windows 7,8, or 10, Linux (Any Distributions), Microsoft® Office 2016/2019
- Speaker, microphone, headgears, web camera, printer or any other extra gadget will be purchased and provided on demand of the user or according to the nature of the work.

The minimum capacity of the desktop must be:

- Core i5, 4^{th} Gen
- 8GB, DDR3 RAM
- Support for USB 3.0 or 3.1 ports
- Optical Drive
- 120GB of SSD
- 500GB of HDD (Depends on the usage or the nature of work)
- GPU (Depends on the usage or the nature of work)

Any change from the above requirements must be authorised by **Assistant Manager IT.**

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 notebooks, laptops, tablets, convertible devices.

Portable computer systems purchased must run Microsoft® Windows 7,8, or 10 and integrate with existing hardware like networking switches, modems, or any other NAS (Network Attached Storage) devices.

The portable computer systems purchased must be HP, Dell, Acer, Lenovo, ASUS, MSI etc.

The minimum capacity of the portable computer system must be:

- Core i5, 4^{th} Gen
- 8GB, DDR3 RAM
- Support for USB 3.0 or 3.1 ports
- Optical Drive
- 120GB of SSD
- 500GB of HDD (Depends on the usage or the nature of work)
- GPU (Depends on the usage or the nature of work)

- Portable devices must have microphone, web camera, built-in Wi-Fi adapter.

The portable computer system must include the following software provided:

- Microsoft® Windows 7,8, or 10, Linux (Any Distributions), Microsoft® Office 2016/2019.
- Installation of any other software will be dependent on the user or on his/her job description.

Any change from the above requirements must be authorised by **Assistant Manager IT.**

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 **Assistant Manager IT.**

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

All purchases of server systems must be supported and compatible with the business's other server systems.

Any change from the above requirements must be authorised by **Assistant Manager IT.**

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 printers, scanners, web cameras, external hard drives, USB flash drives, headphones, microphones, drawing tablets etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or 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 and be compatible with the business's other hardware and software systems.

Any change from the above requirements must be authorised by **Assistant Manager IT.**

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 brands like Apple, Samsung, Xiaomi, OnePlus, Oppo, Redmi, Realme, Lenovo to ensure the business takes advantage of volume pricing based discounts provided by any local retailer in the market.

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

The request for accessories (a hands-free kit, chargers, cables, wireless chargers, Bluetooth headset or air pods etc.) must be included as part of the initial request for a phone.

The purchase of a mobile phone must be approved by Director of the company prior to purchase.

Any change from the above requirements must be authorised by **Assistant Manager IT.**

All purchases of all mobile phones must be supported by official customer service or claimer of the warranty.

All purchases for mobile phones must be in line with the purchasing policy in the Financial policies and procedures manual.

Policy for Getting Software

Policy Code: SSITPL20-SW

Policy Date: 05-11-2020

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 paid software, freeware, open source software must be approved by **Assistant Manager IT** 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 **Assistant Manager IT**.

All purchased software must be purchased from authorized seller or local dealer.

All purchases of software must be supported and compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by **Assistant Manager IT**.

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.

If any open source or freeware software is required, approval from **Assistant Manager IT** 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 **Assistant Manager IT.**

Policy for Use of Software

Policy Code: SSITPL20-SWU

Policy Date: 05-11-2020

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 **Assistant Manager IT** to ensure these terms are followed.

Assistant Manager IT 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.

Skyspin Studios 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 **Assistant Manager IT.**

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 relevant senior person or head of the department.

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

Unless express approval from **Assistant Manager IT** 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 **Assistant Manager IT** 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 **Assistant Manager IT.**

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 **Assistant Manager IT** for approval, responsibility of any damage or loss of the data of the company, or the computer system hardware.

The illegal duplication of software or other copyrighted works is not condoned within this business and **Assistant Manager IT** 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 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 **Assistant Manager IT** 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 **Assistant Manager IT** for investigation and justification about why he/she did not reported to the relevant person.

Bring Your Own Device Policy

Policy Code: SSITPL20-PP

Policy Date: 0-11-2020

At Skyspin Studios 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 Skyspin Studios' 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, or any other gadgets for business purposes. All staff who use or access Skyspin Studios' 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:

- Personal notebooks, smart phones, tablets, iPhone, removable media can be used with in the office, but you need get approval from **Assistant Manager IT.**
- Personal removeable media like USB flash drives, external hard drives or solid states drives are strictly prohibited to be used with in the company.

Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with **Assistant Manager IT** or **Head of the Department** will record the device and all applications used by the device.

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

- Email access, business internet access, business telephone calls etc.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes files related to any project of the company, data of other employees, data of other employee's device, data saved on NAS (Network Attached Storage), data saved on External back hard drives of the company.

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

- To make every reasonable effort to ensure that Skyspin Studios' information is not compromised using 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.

- Not to share the device with other individuals to protect the business data access through the device

- To abide by Skyspin Studios' internet policy for appropriate use and access of internet sites etc.

- To notify Skyspin Studios 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 Skyspin Studios' 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 **Assistant Manager IT** or **Head of the department or any other relevant authority** grants an exemption. Any requests for exemptions from any of these directives, should be referred to the **Assistant Manager IT** or **Head of the department or any other relevant authority**.

Breach of this policy

Any breach of this policy will be referred to **Assistant Manager IT** who will review the breach and determine adequate consequences, which can include for investigation and justification about the breach.

Indemnity

Skyspin Studios 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 Skyspin Studios against any and all damages, costs and expenses suffered by Skyspin Studios 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 Skyspin Studios.

Information Technology Security Policy

Policy Code: SSITPL20-SP

Policy Date: 05-11-2020

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 handy bolt, keypad, lock or Kensington lock etc.

It will be the responsibility of **Assistant Manager IT** to ensure that this requirement is always followed. Any employee becoming aware of a breach to this security requirement is obliged to notify **Assistant Manager IT, Department Head or Any other authorised person** immediately.

All security and safety of all portable technology, laptop, mobiles, notepads, digital notepads, drawing tablets etc. will be the responsibility of the employee who has been issued with the laptop, mobiles, notepads, digital notepads, drawing tablets or any of these. Each employee is required to use security measure like passwords, pattern lock, biometric authentication, physical lock etc. and to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, **Assistant Manager IT** 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, mobiles, notepads, digital notepads, drawing tablets when kept at the office desk is to be secured by passwords, pattern lock, biometric authentication, physical lock.

Information Security

It is the responsibility of **Assistant Manager IT** to ensure that data back-ups are conducted Monday of every week and the backed-up data is kept on WD My Cloud and on External Hard Drives given by the company.

All technology that has internet access must have anti-virus software installed. It is the responsibility of **Assistant Manager IT** 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 permanently terminated from the services and will have to pay the fine as well.

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 device installed in the company.

Each password is to be alpha-numeric and must include one uppercase, one number and a special character and is not to be shared with any employee within the business.

Manager Human Resources 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' then **Manager Human Resources** 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 **Assistant Manager IT** to keep all procedures for this policy up to date.

Information Technology Administration Policy

Policy Number: SSITPL20-AP

Policy Date: 05-11-2020

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 excel file present on the live server. It is the responsibility of **Assistant Manager IT** to ensure that this file is maintained. The file 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.

Assistant Manager IT is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by **Assistant Manager IT.**

Website Policy

Policy Number: SSITPL20-WP

Policy Date: 05-11-2020

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 record up to date will be the responsibility of **Assistant Manager IT**.

Assistant Manager IT will be responsible for any renewal of items listed in the record.

Website Content

All content on the business website is to be accurate, appropriate, and current. This will be the responsibility of **Assistant Manager IT**.

The content of the website is to be reviewed Saturday of every week.

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

- **Assistant Manager IT**
- **IT Director**
- **Assistant Director**
- **Creative Director**

IT Service Agreements Policy

Policy Number: SSITPL20-SAP

Policy Date: 05-11-2020

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.

Where an IT service agreement renewal is required, if the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by **Assistant Manager IT**.

Emergency Management of Information Technology

Policy Number: SSITPL20-EMIT

Policy Date: 05-11-2020

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 **Assistant Manager IT** immediately.

It is the responsibility of **Assistant Manager IT** to take possible action to troubleshoot the problem or error in the event of IT hardware failure.

It is the responsibility of **Assistant Manager IT** 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

If the business's information technology is compromised by software virus or any ransomware attack such breaches are to be reported to **Assistant Manager IT** immediately.

Assistant Manager IT is responsible for ensuring that any security breach is dealt with within 2 hours to minimise disruption to business operations.

Website Disruption

If business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- **Assistant Manager IT** must be notified immediately

__________End__________