

Information Technology

Policy and Procedure Manual

# Introduction

The Al Kathiri Holding 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 Al Kathiri Holding will use to administer these policies, with the correct procedure to follow.

Al Kathiri Holding 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: KATH-IT-001

Policy Date: 1-Jan-2021

## 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

The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

### Purchasing desktop computer systems

The desktop computer systems purchased must run a Windows 10 pro and integrate with existing hardware windows server domain.

The desktop computer systems must be purchased as standard desktop system bundle and must be HP, Dell.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of 14”

* Keyboard and mouse, wired or wireless  Windows 10 pro, Office 2019 plus.

The minimum capacity of the desktop must be:

* Core i7 10th Gen
* 8 RAM
* 1 TB hard disk
* 2 USB
* 1 HDMI port
* 1 Ethernet port

Any change from the above requirements must be authorised by IT manager.

All purchases of desktops must be supported by 2 years warranty 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 notebooks, laptops.

Portable computer systems purchased must run a windows 10 pro and integrate with existing hardware windows server domain.

The portable computer systems purchased must be ThinkPad Lenovo.

The minimum capacity of the portable computer system must be:

* Core i7 10th Gen
* 8 RAM
* 1 TB hard disk
* 2 USB
* 1 HDMI port
* 1 Ethernet port

The portable computer system must include the following software provided:

* Windows 10 pro
* MS office 2019 plus

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

All purchases of all portable computer systems must be supported by 2 years warranty and be compatible with the Alkathiri 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 IT Manager.

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

All purchases of server systems must be supported by 2 years warranty and be compatible with the business’s other server systems.

Any change from the above requirements must be authorised by IT manager.

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, external hard drives etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by IT Manager.

All purchases of computer peripherals must be supported by 2 years and be compatible with the business’s other hardware and software systems.

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

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 Procurement department to ensure the business takes advantage of volume pricing . 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 Apple or Samsung.

The purchase of a mobile phone must be approved by IT Manager prior to purchase.

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

All purchases of all mobile phones must be supported by 2 years warranty requirements here.

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 Number: KATH-IT-002

Policy Date: 1-Jan-2021

## 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 open source, cloud plans, on premise , etc. must be approved by IT manager 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 IT department.

All purchased software must be purchased from The direct owner company.

All purchases of software must be under support.

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

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 IT Manager 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 IT Manager

# Policy for Use of Software

Policy Number: KATH-IT-003

Policy Date: 1-Jan-2021

## 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, then it is the responsibility of IT Manager to ensure these terms are followed.

IT Manager 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.

Al Kathiri Holding 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 Team

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 IT Manager

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

Unless express approval from IT Manager 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 IT Manager 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 IT Manager

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 IT Manager for. The illegal duplication of software or other copyrighted works is not condoned within this business and IT Manager 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 IT Manager for reprimand action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT Manager 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 IT Manager for reprimand action.

# Bring Your Own Device Policy

Policy Number: KATH-IT-004

Policy Date: 1-Jan-2021

At Al Kathiri Holding 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 Al Kathiri Holding'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 for business purposes. All staff who use or access Al Kathiri Holding'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:

* Laptops
* iPhone
* iPad
* tablets

### Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with IT department with HR.

IT 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,
* presentations
* business internet access,.

Each employee who utilises personal mobile devices agrees:

* Not to download or transfer business or personal sensitive information to the device. Sensitive information includes intellectual property, other employee details etc.
* Not to use the registered mobile device as the sole repository for Al Kathiri Holding's information. All business information stored on mobile devices should be backed up
* To make every reasonable effort to ensure that Al Kathiri Holding'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 current operating software, current security software.
* Not to share the device with other individuals to protect the business data access through the device
* To abide by Al Kathiri Holding's internet policy for appropriate use and access of internet sites etc.
* To notify Al Kathiri Holding 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 Al Kathiri Holding'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:

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 CEO grants an exemption. Any requests for exemptions from any of these directives, should be referred to CEO.

### Breach of this policy

Any breach of this policy will be referred to IT Manager who will review the breach and determine adequate consequences, which can include confiscation of the device.

### Indemnity

Al Kathiri Holding 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 Al Kathiri Holding against any and all damages, costs and expenses suffered by Al Kathiri Holding 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 Al Kathiri Holding.

# Information Technology Security Policy

Policy Number: KATH-IT-005

Policy Date: 1-Jan-2021

## 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 separated room.

It will be the responsibility of IT Manager 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 IT Manager immediately.

All security and safety of all portable technology, PCs , laptop, notepads, iPad will be the responsibility of the employee who has been issued with the laptops, notepads, iPads, mobile phones. Each employee is required to use locks, 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, IT Manager will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

### Information Security

All sensitive, valuable, or critical business data is to be backed-up.

It is the responsibility of IT Manager to ensure that data back-ups are conducted daily and the backed up data is kept in company central storage.

All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Manager 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 penalties for violating the confidentiality of information apply.

### Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to set a new password.

Each password is to be letters, numbers and symbols and is not to be shared with any employee within the business.

IT Manager 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 IT Manager 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 |
| Almotakamil Server | IT Manager – Finance Manager |
| Dashboard Server | IT Manager – HR manager – Finance Manger |
| Pbx Server | IT Manager |
| Back up storage | IT Manager |
| Google Workspace | IT Manager |

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

It is the responsibility of IT Manager to keep all procedures for this policy up to date.

# Information Technology Administration Policy

Policy Number: KATH-IT-006

Policy Date: 1-Jan-2021

## 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 IT asset tool. It is the responsibility of IT Manager to ensure that this registered is maintained. The register must record the following information:

* What software is installed on every Hardware
* What licence agreements are in place for each software package  Renewal dates if applicable.

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

A technology audit is to be conducted annually by IT Manager to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to IT Manager

# Website Policy

Policy Number: KATH-IT-006

Policy Date: 1-Jan-2021

## Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

## Procedures

### Website Register

The website register must record the following details:

* List of domain names registered to the business.
* Dates of renewal for domain names
* List of hosting service providers
* Expiry dates of hosting

The keeping the register up to date will be the responsibility of IT Manager.

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

### Website Content

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

All content on the website must follow Alkathiri Holding rules.

The content of the website is to be reviewed weekly.

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

IT Manager – Content Marketing specialist.

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

# PASSWORD POLICY

Policy Number: KATH-IT-007

Policy Date: 1-Jan-2021

## **Purpose of the Policy**

1. **Purpose:** The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

1. **Scope:** The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NIC domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

**3.Policy**

**3.1 Policy Statements**

**3.1.1** For users having accounts for accessing systems/services

* + - 1. Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
      2. All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.
      3. Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
      4. Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
      5. All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.
      6. All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.
      7. Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.
      8. Passwords shall not be revealed on questionnaires or security forms.
      9. Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
      10. The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.
      11. The "Remember Password" feature of applications shall

not be used.

* + - 1. Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
      2. First time login to systems/services with administrator created passwords, should force changing of password by the user.
      3. If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
      4. The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

**3.1.2** For designers/developers of applications/sites

* + - 1. No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.
      2. The backend database shall store hash of the individual passwords and never passwords in readable form.
      3. Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
      4. Users shall be required to change their passwords periodically and not be able to reuse previous passwords.
      5. For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

**3.2 Policy for constructing a password:** All user-level and system-level passwords must conform to the following general guidelines described below.

* + 1. The password shall contain more than eight characters.
    2. The password shall not be a word found in a dictionary (English or foreign).
    3. The password shall not be a derivative of the user ID, e.g.

<username>123.

* + 1. The password shall not be a slang, dialect, jargon etc.
    2. The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
    3. The password shall not be based on computer terms and

names, commands, sites, companies, hardware, software.

* + 1. The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
    2. The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
    3. The password shall not be any of the above preceded or

followed by a digit (e.g., secret1, 1secret).

* + 1. The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# $%^&\*()\_+|~-=\`{}[]:";'<>?,./).
    2. Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

**3.3 Suggestions for choosing passwords:** Passwords may be chosen such that they are difficult-to-guess yet easy-toremember. Methods such as the following may be employed:

* + 1. String together several words to form a pass-phrase as a

password.

* + 1. Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.
    2. Combine punctuation and/or numbers with a regular

word.

* + 1. Create acronyms from words in a song, a poem, or any

other known sequence of words.

* + 1. Bump characters in a word a certain number of letters up

or down the alphabet.

* + 1. Shift a word up, down, left or right one row on the

keyboard.

1. **Compliance** 
   1. Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.
   2. Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.