INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICY FOR THE KIRIBATI AUDIT OFFICE 2023

DOCUMENT OWNER

KIRIBATI AUDIT OFFICE

DEVELOPED AND PROVIDED BY

ICT DEPARTMENT

ISSUED DATE

04 July 2023

Foreword

As the Auditor General of the Kiribati Audit Office, I am delighted to endorse and officially sign the ICT Policy, a significant milestone in ensuring our organization's efficiency and responsible use of information and communication technology (ICT).

In the fast-paced digital age, ICT plays a crucial role in enhancing our capabilities and fostering innovation. However, it also poses inherent risks, demanding a robust policy framework. The ICT Policy exemplifies our commitment to strong controls and best practices, aligned with industry standards and regulations.

After thorough review, I am confident that this policy encompasses the essential principles, guidelines, and procedures for governing our ICT landscape. It defines expectations and responsibilities, promoting a culture of security, privacy, and ethical ICT use.

By adhering to this policy, we aim to enhance data confidentiality, integrity, and availability while ensuring compliance with relevant standards and laws. The policy outlines concrete measures in the following information security domains: access control, asset management, physical and environmental security, communications and operations management, business continuity plan, ICT procurement, and risk management.

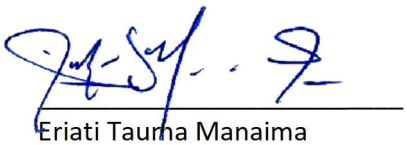
I extend sincere appreciation to Mr. Taukoriri Meita, our Assistant IT Auditor, for his dedicated efforts in crafting this document. His expertise and collaboration enriched the policy, reflecting our organizational needs.

Moreover, I wish to express deepest gratitude to the esteemed review team: Mr. Ruaia Kaburoro (Principal IT Auditor), Mr. Wayne Reiher (MICTTD IT Director), Ms. Nicky Pretorius and her team from INPHYSEC New Zealand, and the PASAI IT Policy Programme team. Their invaluable insights, expertise, and collaborative efforts were pivotal in shaping the policy, ensuring its comprehensiveness and practicality.

I firmly believe that implementing this ICT Policy will safeguard our organization and leverage ICT opportunities. It is the collective responsibility of each member to adhere to its principles, utilizing ICT resources judiciously and upholding our values.

In conclusion, I urge every member to familiarize themselves with the policy, embracing responsible ICT usage, integrity, and accountability.

With my wholehearted approval, I declare the ICT Policy of the Kiribati Audit Office officially effective immediately.



Eriati Tauma Manaima
Auditor General
Kiribati Audit Office
[Date]

Contents

1. Introduction

1.1 Purpose

This policy defines the technical controls and security configurations, users, and Information Technology Administration at the Kiribati Audit Office.

ICT administrators are required to implement and to put into practice what is defined in this Policy to ensure the integrity and availability of the data at Kiribati Audit Office. It serves as a general document policy for KAO in which all KAO employees, contractors and other concerned parties must be familiar with, and define actions and prohibitions accordingly.

1.2 Scope

The scope of this Policy is to ensure data integrity, security, confidentiality, and availability of the Kiribati Audit Office. It is intended to support the protection, control, and management of KAO information assets.

1.3 Acronyms and Definitions

Below is a list of common terms and acronyms that may be used throughout this policy.

AG - The Auditor General.
HODs - Head of Departments.
PITA - Principal IT Auditor
ICT - Information & Communication Technology (Technician). Sometimes referred to just IT.
EA - Executive Assistant.
External Media - i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, Thumb drives, tapes
Firewall - a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
VPN - Virtual Private Network
Internet Bottleneck - When multiple devices connected to the internet simultaneously will create a slow internet speed, especially if the devices are wireless.
LAN - Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
Login ID - is a unique Identifier that granted to each user from the system to access computer system or work network.
MICTTD - Ministry of Information, Communication, Transport and Tourism Development of the Government of Kiribati
Peer-to-Peer - computer system which are connect to each other via Internet.
SAI – Supreme Audit Institution
Virus/Malware - a malicious software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

1.4 Applicable Status/Regulations

This policy is created based on the existence of the Kiribati Government regulation for the use of computer systems and to support confidentiality of data. Below are some of the related acts and policies for the use of computer system.

i) Telecommunication Act: Part VII – Computer Misuse
ii) Ministry of Information, Communication Transport and & Tourism Development – National ICT Policy 2019 EMPLOYEES
iii) Cybercrime Act 2021
iv) Communications Act 2013

2. Human Resources Security

2.1 Employee Requirements

The first line of defence in data security is the individual of KAO Staff. KAO Staff are responsible for the security of all data which may come to them in whatever format. The ICT Staff is responsible for maintaining ongoing training programs to inform all users of these requirements.

a) Wear Identification Badge/Card so that it may be easily viewed by others – to help maintain KAO building security, all employees should prominently display their employee identification Cards during working hours. Visitors should wear a Visitors ID Card to enter the building.
b) Challenge Unrecognized Personnel – It is the responsibility of all audit personnel to take positive action to provide on-site security. KAO Employees should question non-employees who enters the building without a Visitors ID Card and challenge them as to their right to be in the building and report the issue to management.
c) Computer Literacy and Lending Assignments – All staff except Cleaners and Drivers are entitled to a Laptop/Desktop computer which is assigned by the ICT Section after the computer is fully checked for any damages or system errors. This applies to brand new and used computers. Employees are required and expected to be computer literate. Since these computers are recorded in the database after they have been assigned to the staff, the assigned Staff takes full responsibility on taking care of the computer. Refer to ***Annex A, B, I***
d) Employees may be allowed to borrow tools and equipment from the ICT department for work related purposes or for other reasons with the approval of the ICT department. The staff is required to know how to use the tool/equipment and should be aware that it will be assigned under his/her name in the database for record until he/she returns it. The staff takes full responsibility of the tool/equipment while under his/her care.
e) Caring of Laptops & Desktop Computers – All employees should follow the guideline on how to take care of the computers assigned to them especially Laptops if the staff is entitled to take it home. Staff must follow the guideline on "How to take care of Laptop" see ***Annex B.***
f) Caring of ICT Equipment & Devices – All employees should follow the guideline on how to take care of ICT Equipment & Devices. See ***Annex C.***
g) Medically Fit and Fully Alert – all employees are required to be medically fit and fully alert of their surroundings during working hours. This will enable staff to react quickly to safety in case of hazardous emergency that might happen during working hours.
h) All KAO Employees are required to Accept All Conditions of this Policy – All Employees are required to fully Understand and Accept All Conditions of this ICT Security Policy.

2.2 Prohibited Activities

KAO Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities may be referenced elsewhere in this document.

- Employees are not allowed to leave the office open – after late working hours.
- Eating/Drinking while working on a computer is not encouraged – tiny pieces of food can break off and spilling/dripping of drinks might fall/spill into computer keyboard and surroundings that will attract insects like ants to infest the inside of the computer sensitive electronics and pest like rats to chew on power supply chords. If the staff should eat while working, he/she will make sure that no problems mentioned should be caused by such action.
- Opening the Computer casing – is strictly prohibited. Only ICT Staff can open the laptop hardware cover/casing for maintenance and repair purposes only.
- Crashing an information system – Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, however, a repetition of such action by the user may be viewed as a deliberate act if never reported. Not only will this action goes against the policy, but it will also become a criminal action that needs to be dealt with in court as per the new Cybercrime Act 2021.
- Attempting to break into an information resource or to bypass a security feature is strictly prohibited. This includes running password-cracking programs or sniffing programs and attempting to circumvent file or other resource permissions. This is also a crime under the new Cybercrime Act 2021.
- Browsing – The wilful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software – Use of personal software is prohibited. All software installed on KAO computers must be approved by ICT Manager. Staff computers are configured so that they have limited capacity to install executable files except for administrators, therefore – having a software installed that is not approved by the ICT Manager is a result of a deliberate bypass of the security system of the computer.
- Software Use – Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the KAO is strictly prohibited.
- Sharing/Loaning of User Login Credentials – sharing of user password is prohibited, each user is not allowed to give or pass his/her password used in the office to others.
- Computer Settings – Staff can only change the settings of the computer if there are no restrictions on that setting. Restricted computer setting change will require an Administrator (ICT Staff) to approve the change. A change in a restricted computer setting without the knowledge of an Administrator will be treated as a deliberate bypass of a security feature by the user.
- Computer Repair & Maintenance – Employees should only give their computers for maintenance and repair to KAO ICT Staff Only.

2.3 Internet Access/Usage

Internet Access is provided for KAO and is considered a great resource for the Office to carry out its functions and communications.

Multiple access to the internet at once by different devices will consume a lot of bandwidth which may lead to slow internet speed. To minimize the internet **bottleneck** and maximize internet

capacity, internet access is controlled by a Firewall Filter which manages the internet usage and traffic.

KAO INTERNET INFORMATION

Internet Service Provider: Starlink
Satellite Link: Starlink
Internet Monthly Cost: $431.25
Internet Download Speed: avg 200 Mbps
Internet Upload Speed: 15 Mbps
STAFF GROUPS AND THEIR RULES & SPEED ALLOCATION

GROUP	RULES	SPEED Download/Upload	Schedule
Administrators	No-Rules	Max/Max	24hrs
Video Calls	Certain Websites blocked	Max/Max	24hrs
Training	Certain Websites blocked	128KBps/128KBps	24hrs
HOD	Certain Websites blocked	96KBps/128KBps	24hrs
Senior & Privilege	Certain Websites blocked	64KBps/128KBps	24hrs
Junior	Certain Websites blocked	32KBps/128KBps	24hrs

The Internet Access provided should be used for official purposes only and not for entertainment or any other non-official business. ICT Staff have blocked "Certain Websites" that are known to consume a lot of bandwidth and are not work related and will continue to update this list of blocked websites from time to time. Request for access to such websites may be granted given there is a good reason for such request.

Users must be aware that internet usage is monitored and logged, if an employee is found to be spending excessive amount of time in consuming large amount of bandwidth for non-work-related use, disciplinary action will be taken.

2.4 Reporting Software Malfunctions

Computer Users should inform the ICT personnel when the user's software does not appear to be functioning correctly. The malfunction – whether accidental or deliberate – may pose an information security risk. If the computer user suspects a computer virus infection, the user should take these steps immediately.

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs
- Do not turn off the computer or peripheral devices
- If possible, physically disconnect the computer from the network to which it is connected
- Inform the ICT personnel as soon as possible. Write down any unusual behaviour of the computer (screen messages, unexpected disk access, unusual responses to commands, etc) and the time when it happens.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ICT personnel should monitor the resolution of the malfunction or incident, report the result and action with recommendations on steps to avert future similar occurrences.

2.5 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting the audit, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the audit and hold all data in the strictest confidence manner. Any purposeful release of data to which an employee may have access is a violation of KAO ICT Security Policy and will result in disciplinary action which may lead to legal action.

2.6 Transferring Software and Files between Home and Work

Personal software shall not be used on KAO Computers or Networks. If there is a need for a specific personal software to be installed on KAO Computer, user should submit a request to the ICT department's Head for approval. Users shall not use KAO purchased software on home or on non-audit office computers or equipment. All Audit work should be done on the audit office equipment only. ICT System information, Financial Information or Human Resource data shall not be placed on any computer that is not the property of the audit office without the consent of the respective head or supervisor. It is crucial to the audit office to protect all data and to do that effectively we must control the system in which is contained.

2.7 Data Security Protection

It is essential that the SAI's crucial data is secured at all costs. Hence, all official computers, servers and devices that stores SAI's data should have security mechanisms in place which include the following:

- Logins: All Computers must be protected with a password to prevent unauthorised access critical data in the computer.
- Lock Screen: Computers must be configured to be locked after a few minutes of inactivity. This will require a re-login to the computer.
- User Data backup: All staff are required to back up their own data using the "Storage" partition on their computers, or by using the Server's Network shared drives provided for them.
- Hard Copy work papers: Staff should NEVER leave paper records around their working area or anywhere for anyone to see especially if the paper contains sensitive information. All work paper records should be kept in a locked file cabinet when it is not used.
- Sending Data outside the Office: Staff should not give or transfer any audit sensitive information to anyone by any means without the written approval of their supervisor.
- Virus Protection: To prevent data loss/theft from viruses, the Antivirus installed on KAO Computers must all be active and updated to their latest update definitions regularly.
- Server Backup: Server should have two backups that runs daily. One backup should be within the Server for easy access, and another backup of the same data should be in a remote offsite area for recovery unexpected office disasters, etc.
- Computer Maintenance Schedule: To prevent data loss if the computer should fail unexpectedly, IT Staff should perform a maintenance on a scheduled basis (Check ***Annex G*** for such Schedule and procedure).

3. Access Control

3.1 User Access Management

3.1.1 Login Credentials

Individual users shall have unique logon IDs and Passwords to KAO ICT Systems. An access control system shall identify each user and prevent unauthorized users from entering or using official information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier
- Users shall be responsible for the misuse of their individual logon ID

All user login IDs are audited at least once a year and all inactive login IDs are revoked. The Registry Clerks or Office Manager should notify the ICT Department/Personnel upon the departure of all employees at which time login IDs are revoked.

3.1.2 Password management

User IDs and passwords is a requirement to access the Office Network and Resources, office Computers and Devices such as Printers etc. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Passwords must be changed every 6 months.

Office password requirement – Passwords should have minimum of 8 mixed characters of upper- and lower-case alphabets, numeric and symbols characters.

Restrictions on Sharing Passwords – Passwords must be kept confidential and out of sight.

Password Reset – If the user does not have restrictions on resetting his/her password, they may do so if they think the password has been compromised. However, if they do not have access to reset their password due to restrictions, they may inform ICT Personnel for assistance.

3.1.3 Attendance management

KAO Staff attendance is being monitored and controlled with the Fingerprint Attendance Punch Machine. All KAO Employees should be registered on this device. This will allow management not only to monitor staff attendance but also to keep track of staff movement as part of a security measure. The Office Manager is responsible for monitoring and keeping track of staff attendance while ICT Staff are responsible for the Attendance system configurations and maintenance. All staff are required to punch in and out before and after work.

3.2 Network Access Control

3.2.1 Network Shared Folders & Printers Access

Network Folders are hosted on the KAO Server and with the Server's Active Directory feature; Employees are assigned Network Access to Shared specific Network Folders according to their department and their Post Positions.

Employees can view the entire Network Folders/Printers infrastructure but will be limited to only what their Read/Write privileges had been assigned to them to open certain Folders or add certain Printers.

Table1: The table below depicts the user access right to a Department Network Folder.

Network Shared Folder	Users with Read/Write Access
Central Government	ICT Staff, AG, Department Members only
Local Government	ICT Staff, AG, Department Members only
SOE	ICT Staff, AG, Department Members only
Projects	ICT Staff, AG, Department Members only
ICT	ICT Staff, AG, Department Members only
Human Resource	ICT Staff, AG, Department Members only
Registry & Corp Services	ICT Staff, AG, Department Members only
Account	ICT Staff, AG, Department Members only

Table 2: The table below depicts the user access to a non-Department Network Folder.

Network Shared Folder	Users with Read Access Only	Users with Read/Write Access
Shared	All Staff	
Resources	All Staff	ICT Staff
Scans	All Staff	
HOD	HOD Staff & ICT	
Database	ICT, AG & Registry Staff	
Training	AG	Staff undertaking Training & ICT
Social Committee	All Staff	Social Committee staff
Work Folder/username	Specific to each staff.	

Table 3: The table below depicts the user access to Network Printers

Network Shared Printer	Users with Print/Scan/Copy Access
OKI Laser Colour Printer ES8473 MFP	All Staff
Brother Laser Mono Printer HL-L2350DW	All Staff
Brother Inkjet Colour Printer MFC-J480DW	ICT & Registry Staff
Brother Laser Colour Printer MFC-9140DN	ICT & AG

Network Shares Management

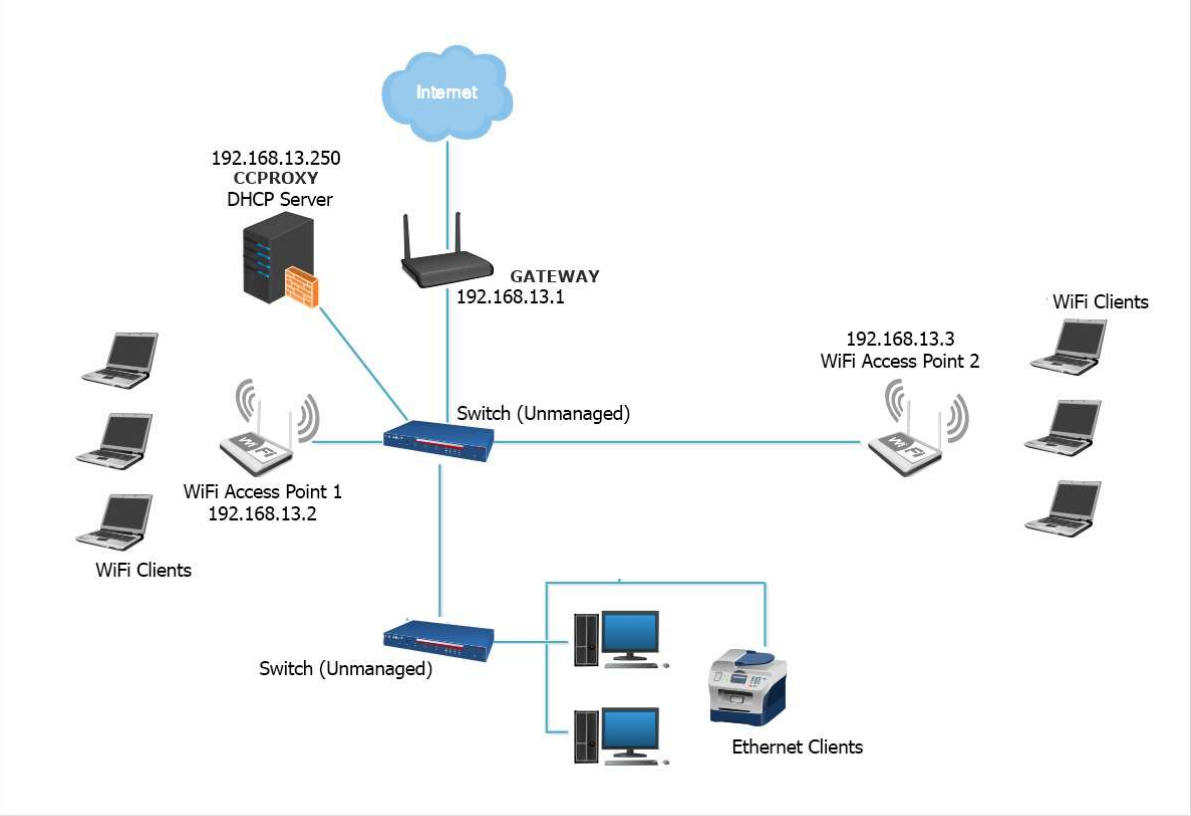
- Editing or Deletion of Network files is monitored and logged for Audit to allow reviewing of any Network Files modification and deletion by any user and when.
- Media Files specifically audio and video formats cannot be saved on certain Network Shared Folders, except for the ones that requires them.
- The use of Printers is also logged to enable a review of how much printing is done on a daily/monthly basis by each user.

3.2.2 Network Connectivity

The ICT Department of the Kiribati Audit Office must provide a secure network for audit work, research, administrative needs, and services.

Below is the KAO Network Infrastructure diagram:

Diagram 4.a



Internet Access via diagram above: The Gateway is configured so that it only allows the Server to access the Internet. A Firewall (ccproxy) is installed on the Server to manage connected Network Devices access to the internet. All Network Devices can access the Internet ONLY by going through the ccproxy Firewall. (refer to Section 2.3 for more information).

3.2.3 Appropriate Connection Methods

KAO devices – computers, laptops and other devices connections may connect to KAO Network at appropriate connectivity points wirelessly or with ethernet cable.

Only KAO Devices should connect to KAO Network – connecting to KAO Network with non-official Devices is prohibited. For Safety measures, connecting of other devices including personal mobile phones and other electronic media to KAO Network should be approved by the ICT Department.

3.2.4 Network Registration

Every device connected to KAO Network should be registered with the ICT Department to keep record on the Device's details and the owner of the device.

3.2.5 Responsibility for Security

Every Computer or Device that is connected to the KAO Network has an associated owner. For the sake of this policy, the owner is referred to the staff of the Audit Office. Each staff need to ensure that their computer or devices that connect to the network are secure from any Virus Attack. There should be an Antivirus installed and running.

3.2.6 Computer Security Standard

These are the security standards for all staff Computers that are connected to the KAO Network.

- Every installed Software in a computer must have a genuine license.
- Every computer must have an active and updated Antivirus
- Every computer must meet the minimum hardware specification: see ***Annex D.***
- Every computer must go through a maintenance procedure Scheduled by ICT Department. See ***Annex E*** for Maintenance procedure.
- ICT Department will provide consultations on request to staff who would like more information on security measures.

3.2.7 Protection of the Network

KAO ICT Department reserves the right to restrict certain types of traffic coming into and across the KAO Network. The ICT Department filters or restricts traffic that is known to cause damage to the network through firewall and other security measures.

4. Asset Management

4.1 Office Database

The Kiribati Audit Office should have a running Database that capture what is needed to be on record by the office. It should be available and accessible locally and remotely to all staff with different access privileges implemented by the Database Developer (ICT Department) with the approval of the Auditor General.

The Database system should be maintained and upgraded regularly in design and security by the Database Developer. Record Entry shall be done by the assigned Human Resource (HR) Staff, Registry Staff, Accountant, and ICT Staff.

4.1.1 Database requirement.

The Database should meet the requirements below.

- Platform – Any database platform that can be managed by ICT Developer with features written below.
- Design/Interface – should be clean and easy to navigate
- Content – any official data that needs to be on record should be included in the database.
- Access – all staff should be able to access the database simultaneously, locally, or remotely.
- Security – all Access should be restricted depending on the user's privilege.
- Platform – should be cost effective, scalable, secure, and easy to use.
- Host – cost effective, fast, trusted, secure and excellent support

4.1.2 Database Configuration

All configurations below should be checked and approved by the Auditor General.

a) Platform used: Filemaker Pro & Filemaker Server: FileMaker is a cross-platform relational database application from Claris International. It integrates a database engine with a graphical user interface (GUI) and security features, allowing users to modify the database by dragging new elements into layouts, screens, or forms.
b) Office Database Content:
    a) User Profile – This includes Personnel Details, Leave & Attendance, Office Assets, Event Participations, etc.
    b) Registry and Administration – Filing System, PFs, Approved Holidays, etc.
    c) Account Section – Asset Register
    d) ICT – ICT Works, maintenance schedule, etc.
    e) Audit Works – Contains all audit records, procedures from beginning to end.
c) Account Security: The Database should be able to log all user activities within the database. Users must be categorized into different privilege access. Below is the type of users.
    d) Administrators – Full Access
    e) Human Resource – Enter/Modify HR Records.
    f) Accountant – Enter/Modify Account Records
    g) Registry & Admin – Enter/Modify Registry & Admin Records
    h) KAO Staff – Can only view his/her record plus other allowed records from other Layouts.
i) Access & Hosting: The Database should be hosted on a dedicated server or in a cloud-based system. Users will be able to access the Database simultaneously locally and remotely.

As for tracking changes in the management of the database. As mentioned in Section 12.1.a of this Policy, it is not necessary to track changes in a written manner since the database itself should be able to present/show all configurations, logs, and changes.

4.2 Office Website and Social Media page

The Kiribati Audit Office should have a running Website and a Social Media page that reflect and summarise how the Office carry out its duties. The content of such online platforms should be updated regularly and available for public viewing.

4.2.1 KAO Website

The purpose of the KAO Website is to define the Office vision, mission, and its values to the public online. The content should contain only what is needed for public viewing and should be updated regularly. Below is a list of the Office website requirement.

- Design/Interface – should be clean and easy to navigate
- Content – should be readable, accurate and updated regularly
- CMS (Content management system) – cost effective, secure, scalability and easy to use.
- Host – cost effective, fast, trusted, secure and excellent support

4.2.2 Social Media

The Office should also have a social media page whether be Facebook, Twitter, LinkedIn, etc. The purpose of having a social media page is to boost visibility since almost all online users have a social media page which makes it easier for the office to reach people online if it also utilizes such platform. Below is the office Social Media page requirement.

- Design/Interface – should be a business version of the used Social Media Platform
- Content – Official News, Events and Announcement to/for the public. This content should be linked to the official website. The content should be provided by the concerning Section or Staff and will be uploaded by the Administrator of the Platform.
- Social Media Platform – the office should focus on using the same Platform(s) that most of its clients are using.
- Management – ICT Department should create the official Social Media Account and Page and should manage its settings, configurations, security and contents.

5. Physical and Environmental Security

5.1 Secure Areas

Physical Access is the second line of defence in accessing KAO Computer resources This policy is designed to provide building access in a secure manner. Below is a list of access control of KAO building.

- All doors of the audit office should be locked when the office is not being used for official business by staff members.
- Entrance of the building during non-working hours is not allowed unless there is an approval from the AG. Entering of KAO premise without the AG's knowing is strictly prohibited.
- The door to the IT Room (Server), AG, EA rooms should always be locked when it is not being occupied. During working hours, visitors to these rooms wait at the waiting area at the reception.
- The reception area is always staffed, during working hours 9:15am to 5:15pm. Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk and wear a visitor ID Card.
- The building should be equipped with security cameras to record activities within the office encompassing the front entrance. These cameras should cover all areas of the office indoor and outdoor and should be recording 24hrs.
- All KAO Windows must be securely secured with security wires.
- All electrical and network cabling should be raised above to prevent electric shock from water floods.
- Fire-Extinguishers should be placed in the Office and staff should be trained to use it to prevent fire hazards if it should happen.

5.2 Equipment Security

All ICT Hardware (Equipment) must be protected physical and environmental threats. Intentional or unintentional incidents that my lead to damage of equipment should be prevented at all costs. Please refer to "2. Employee Awareness and Responsibilities".

5.2.1 ICT Equipment

This equipment include, servers, routers, switches, cameras, printers, etc.

- Equipment processing sensitive information should be protected to minimize the risk of information leakage due to emanation.
- Equipment should be protected from power failures and other disruptions using an uninterruptible power supply (UPS) or power surge power boards.

5.2.2 Computers and laptops

Please refer to the guidelines in ““ANNEX B: Caring of Laptops/Desktops” for more details.

5.2.3 Disposal of Portable Media Storage

It must be assumed that any external media in the possession of an employee is likely to contain either protected audit information or other sensitive information. Accordingly, Portable Media Storage such as CDs, DVDs, diskettes, USB flash drives, External Hard Disk, etc should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be disposed and to utilize this policy in its destruction.
- Portable Media Storage devices should never be thrown in the trash.
- When no longer needed, all forms of external media are to be sent to the IT department, while the IT department will check and consult the Account Section for proper write-off and disposal.

5.2.4 Disposition of Excess Hardware

As the older computers and equipment and other ICT devices are replaced with new systems, the older ones (not necessarily broken) being replaced are held in the ICT Inventory for a wide assortment of uses:

- Spare parts: the ICT Inventory of the replaced computers, equipment and other ICT devices can be used as spare parts for the new ones.
- Emergency replacement basis: If the current new device encounters an unexpected problem with limited time to fix, the old working devices may act as a temporary replacement.
- Testing Environment: Old working computers are useful to run test on new software, new system configurations, etc. before application on current devices or system is implemented.

5.2.5 Disposal of Paper

- Paper disposal: All papers which contains sensitive information that is no longer needed must be shredded before being disposed. The preferred method of disposal is to be burned. Staff should not place these sensitive papers in a trash container without shredding.

5.2.6 Lifespan of ICT Equipment before disposal

All ICT Devices must be replaced whether they are broken or not. Almost all new technology releases are backward compatible with older technology, but not always old technology will be compatible with the latest technologies in terms of hardware and software. So, for the office to stay compatible with the latest trend in technology, if the device reached its maximum upgrade software/hardware wise, it must be written off regardless of whether it is broken or not and to be replaced with a newer version of the device. For more detail on each device lifespan, refer to ***Annex H***.

6. Communications and Operations Management

6.1 Change Management

Changes to information processing facilities and systems should be controlled and documented. Operational systems and application software should be subject to strict change management control.

In particular, the following items should be considered

- Identification and recording of significant changes to critical ICT Equipment such as Servers, routers, computers, etc.

- Assessment of the potential impacts, including security impacts, of such changes.

- Communication of change details to all relevant persons.

- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.

6.1.1 Log Management

Statement of Policy

To ensure that KAO is tracking changes to networks, systems and workstations including software releases and software vulnerability patching in information systems. Change tracking allows the Information & Communication Technology ("ICT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT Staff who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system
    a. When Changes are tracked within a system, i.e., Windows updates in the Add or Remove Programs component or electronic audit record (EAR) updates performed and logged by the system, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process if the change causes an adverse effect within the system and needs to be removed.

6.2 Information System Activity Review

Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. An Audit Shall be conducted on a regular basis of records of system activity to minimize security violations.

Procedure

1. The ICT Audit Department shall be responsible for conducting reviews of KAO's information system activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
2. The Assistant IT Manager shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
3. Audit shall be conducted if there is a suspicion of wrongdoings. In conducting these reviews, the ICT Department shall examine audit logs for security-significant events including, but not limited to the following:
    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, unauthorized access, etc.
    b. File access – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access and unauthorized file creating, modification or deletion.
    c. Security incidents – Examine records from security devices or system audit log events that constitute system compromises, unsuccessful compromise attempts, malicious logic, denial o service, or scanning/probing incidents.
    d. User Account – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have access to the information or the system.

The ICT Department shall forward all completed reports, as well as recommended actions to be taken in response to findings, to Office Management for review. The ICT Principal Auditor shall be responsible for maintaining such reports. The PITA officer shall consider such reports and recommendations in determining whether to make changes to KAO's administrative, physical, or technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy referred in Section 2. Employee Awareness and Responsibilities.

6.3 Malicious Code

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.

- Viruses can damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.
- Worms are a type of virus that self-propagates from computer to computer. Its functionality is to use all your computer's resources, which can cause your computer to stop responding.
- Trojan Horses are computer programs that are hiding a virus or a potentially damaging program. It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software, instead the program is performing malicious actions on your computer.
- Malicious data files are non-executable files—such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file—that exploits weaknesses in the software program used to open it. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing the files via email, social media, and websites.

6.3.1 Controls against Malicious Code

KAO follows these security practices to help reduce the risks associated with malicious code:

- An antivirus is installed and updated regularly on all KAO Computers.
- Emails and Attachments are scanned using Email host built in virus scanner. Staff should report and seek advice on suspicious emails and attachment to ICT Departments for proper action.
- Employees should Avoid or Block pop-up advertisements while browsing the web. An adblocker browser extension is installed by ICT for all user computers.
- Portable Media Storage Autorun and Auto-play features are disabled.
- Users should change their passwords if it is believed that their computer is infected with virus. This includes any passwords for websites that may have been cached in your web browser.
- Keep software updated. Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available. (See Understanding Patches and Software Updates for more information.)
- User Back up data. Beside the Server backup, Staff are encouraged to regularly back up their work documents, photos, etc to the provided "Storage" partition on their computers, on an external hard drive or on a cloud storage to prevent unexpected data loss.
- Install or enable a firewall. ICT Staff are to install/enable a Firewall for the Entire Network and on a Staff Computer for extra security.
- Use anti-spyware tools. Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.
- Monitor accounts. Look for any unauthorized use of, or unusual activity on, your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.

- Avoid using public Wi-Fi. Unsecured public Wi-Fi may allow an attacker to intercept your device's network traffic and gain access to your personal information. See Section: 8.1 Public Wireless Usage standards and Policy for more details.

6.4 New Software Distribution

Only software that approved by the IT Department should be used on KAO Computers and networks. A list of approved software is maintained in ***Annex F***. All new software will be tested by IT Staff to make sure compatibility with Office requirement. In addition, the IT Staff must scan all software for viruses before installation.

All data and program files that have been electronically transferred to the audit office computer or network from another location must be scanned for viruses.

Every portable media is a potential source for a computer virus. Therefore, they should all be scanned for viruses before it is used on Office Computers.

Computers shall never be "booted" from a portable media. Users make sure that no portable storage devices are connected to their computers before booting (powering up) their computers. This is to make sure that any hidden auto start-up viruses don't become active when booting a computer.

7. Specific Topic on Protocols and Devices

7.1 Public Wi-Fi Usage Standards and Policy

Due to the convenience of Public wireless access points in hotels, airports, cafes, etc. it has become imperative that this policy should outline the process and procedures for acquiring wireless access usage on Public Wi-Fi.

Usage of Public Wi-Fi requirements: All staff Wi-Fi devices such as Laptops and smart devices should meet the following requirements to make Public Wi-Fi.

- The device should have an antivirus installed, active and updated.
- The Operating System of the Device should be of the latest version.
- The Internet Browser should be updated to the latest version.
- Upon connection, if there is an option; the user must configure the device to set the connection type to a Public Network so that the device treats the connection as such by automatically adding a few more layers of security on the device via the connected network.
- Staff should be cautious when using Public Wi-Fi by sticking to just what needs to be done online and not browse/surf other unnecessary websites beside work stuff.
- Connected Devices should not stay connected for long hours. They should be disconnected if it is no longer needed.

If the Staff user's Wi-Fi device does not have these features or is unable to follow the above requirements, should notify the IT Staff.

7.2 Use of Portable Media Storage

Portable Media storage included within the scope of this policy includes, but is not limited to, SD Cards, DVDs, CDs, USB Flash drives, External Hard Disk.

The purpose of this policy is to guide KAO employees of the Practice in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from

different locations. Every office computer is presumed to have sensitive information stored on its hard drive; therefore, procedures must be carefully followed when copying data to or from portable media to protect sensitive data. Since portable media, by their very design are easily lost, care and protection of these devices must be addressed.

The use of Portable Media device in various formats is a common practice within any workplace. All KAO Users must be aware that sensitive data could potentially be lost or compromised when moved (cut/paste) from the office system/network.

Portable Media device received from an external source could potentially pose a threat to the Audit computers and Network, since it has been known to be a very good source of virus/malware to be transmitted to different computers.

For proper protection from such threats with the use of Portable Media devices; it is recommended that:

- All Portable Media devices that belong to KAO should be kept and maintained by IT Department.
- Office and Personal portable media devices should be scanned every time after every usage from an external source.

8. Business Continuity Plan

Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, system failure, natural disaster) that will cause damage to the overall ICT System.

The Audit Office is committed to maintaining formal practices for responding to an emergency or other occurrence that damages the overall ICT System. The audit office shall continually assess potential risks and vulnerabilities to protect audit information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

Procedure

1. Data Backup Plan – Backup procedure of the overall ICT System should be automated daily to an extra physical Storage Hard Drive within a Server and to an offsite Storage outside the office or in the Cloud.
2. Remote Access – In case of Office Lockdown due to a pandemic (e.g., Covid19), all staff should be able to Access Office Resources using a secured Virtual Private Network (VPN), Secure FTP or other Remote Access means. Staff can also utilize the use of Video/Call and Chat communications using Video Call apps like Zoom or Teams or Facebook Messenger and the use of Official Email.
3. Environmental Disaster – A spare/secondary Physical Server, Network devices such as Network Switch and Wi-Fi Access points should be placed in an offsite location and should always be on standby if there should be a full damage on all ICT Devices in the office due to Natural Environmental Disaster.

ANNEX A: Laptop Lending & Usage Agreement

KAO Laptop Lending & Usage Policy

Purpose: This policy establishes the rules and responsibilities for the lending and use of laptops provided by KAO. This policy applies to all active KAO staff.

Responsibility: All KAO staff are responsible for keeping the provided laptops safe and in good condition. If damages are incurred, the staff member is responsible for all charges as applicable. Intentional vandalism will result in being charged up to the full replacement cost of the laptop. The laptop always remains the property of KAO.

Policy Rules:

- Laptops are provided and maintained by the KAO IT Staff. If staff experience problems with the laptop, they should consult with the KAO IT Staff regarding the matter as soon as possible.
- Staff members are responsible for ensuring that the laptop is not damaged, lost, or stolen while under their care. The replacement fee for the laptop is subject to the cost of the laptop when first purchased. A certified copy of the original invoice is kept with the IT/Account section for reference. In circumstances where a laptop part is damaged, the staff member is liable to pay for the part to KAO. The values of all KAO laptops are degraded by 25% each year.
- Laptops are intended ONLY for KAO active staff and work-related use.
- Prior to borrowing the laptop, both the staff and IT staff will ensure that all laptop components (cable, power adapter, etc.) are present and recorded.
- Laptop users are not allowed to install additional software/programs besides the ones pre-installed by the IT staff unless authorized by a superior and checked by IT staff.
- Laptop maintenance will be carried out from time to time, and users will be advised by IT staff in advance prior to conducting the maintenance. Laptop users are responsible for backing up their personal files and may contact IT staff for assistance if necessary. IT staff will not be held responsible for the loss of the user's personal files during maintenance.
- All KAO laptops have an Administrator account managed by IT staff and a standard account for the user of the laptop.
- Laptop use is a privilege that will be revoked if the service is abused.
- Laptops must be returned, checked, logged, and reconfigured by the IT section prior to lending them to another user.

Penalties:

- KAO IT Staff, in conjunction with Heads of Departments (HODs), will discuss and enforce other necessary penalties if the replacement fee is not applicable.

Agreement:

By being employed at KAO, staff members agree to:

- Abide by the policies as stated and referenced above.
- Pay full repair and/or replacement costs in the case of damage, theft, or loss.
- Implementation and Enforcement:

This policy is effective immediately and will be enforced by the KAO IT department and respective Heads of Departments (HODs). Non-compliance with this policy may result in disciplinary actions including but not limited to revocation of laptop privileges.

For any issues or concerns related to this policy, please contact the KAO IT department.

ANNEX B: Caring of Laptops/Desktops

It is important that you take good care of your computer to keep it working well. Following these easy steps will ensure that your computer lasts longer and requires less maintenance. As a bonus, many of the steps will also maintain your computer's speed. It is also useful to give up your Computer to ICT Staff as part of their schedule routine to do a full maintenance of the computer occasionally to remove any errors or problems which might have crept in during the routine usage.

Steps:

1. Keep liquids away from your computer
2. Always have an antivirus installed and active with the latest updates.
3. Always keep the Operating System and installed programs up to date.
4. Avoid installing Pirated Programs that uses cracks to bypass genuine licensing.
5. Keep food away from your computer
6. Do not use your computer in a room where animals are.
7. Ideally keep the computer in a clean and dust free room and a well-ventilated area.
8. Always have clean hands when using your computer.
9. Protect the LCD display monitor by avoiding hard and heavy objects that will put pressure on the screen that will eventually damage it. Also handle the screen lid gently when opening or closing.
10. Hold and lift the computer by its base, not by its LCD display (the screen).
11. Keep the power cord and connected cables safe when plugged in by keeping it tucked away from your working area.
12. Don't roll your chair over the computer cord and other connected cables.
13. Be sure to plug accessory devices into their proper slots.
14. Handle any removable drives with care when plugging or inserting/removing them and make sure that they are inserted at the correct angle.
15. Don't leave your computer in a place where it could be easily stolen.
16. Have the unit cleaned on a schedule basis to remove internal dust.
17. Protect or don't use your computer in areas that is proximity to the sea or humidity.
18. Place a Laptop in a Laptop case/bag to reduce the risk of damage when bumped or dropped.
19. Only use and store your computer in a well-ventilated area.
20. Use a cleaning brush (or an old toothbrush) to clean the area around the exhaust fan screen to get rid of the accumulated dust to keep the air flow going and prevent overheating.
21. When using the computer, place it on a hard, flat, and clean surface.
22. Avoid opening multiple programs and files at the same time, always close the ones that are not being used.
23. Avoid downloading and running executable files from the internet or from external sources. Confirm with ICT Staff if you should do so.
24. A system drive (C: Drive) will not exceed 75% of used storage.
25. Do not try to open the cover of the computer to expose the inside components.
26. Do not miss the Maintenance Schedule provided by the ICT Department.

While staff can follow the guidelines provided above maintain their own computers. The ICT Department also have a schedule on all KAO Computers for maintenance. Each staff in possession of a computer will have their turn for maintenance provided in the Schedule. It is important that they do not miss this Maintenance Schedule to prolong the lifespan of their computers.

ANNEX C: Taking Care of ICT Devices

Follow these steps in maintaining the ICT Devices mentioned below: If a staff cannot do any of the steps written, then it is meant for ICT Staff, otherwise all staff should put these steps into practise.

Inkjet Printers

- Use the printer frequently to prevent the ink in the cartridge from drying.
- Frequently run a maintenance feature on the printer to keep the printer head clean
- Take caution when replacing the printer cartridges and only use genuine cartridges.
- Keep the printer clean and dust free, make sure no obstacles are in the way when printing
- Use the latest software and drivers for the printer

Laser Printers

- Protect yourself - Make sure you turn off and unplug your printer before cleaning it up to avoid any kind of electrocution. Also, wear a mask and latex gloves to prevent the fine toner particles from sticking on your skin or getting into your lungs.
- Always keep the Printer's manual and use it when conducting a maintenance on the printer.
- Remove Dust and Debris by using proper cleaning tools (small, pressure-controlled vacuum, moist cotton swabs, etc).
- Take caution when replacing the Toners and only use a genuine Toner.
- Use the latest software and drivers for the printer

Network devices (Wi-Fi Routers, Access Points, Network Switches, NVR, Video Conference Devices)

- Use the latest firmware
- Reboot (Restart) regularly
- Place it in an optimal area safe from public reach
- Run its cables off the floor and using cable covers/protectors
- Always keep it clean from dust

USB Keyboards and Mice and Portable Storage

- Run USB cable safely to avoid bending and stress when heave objects are placed on or around it.
- Avoid Liquids near the device
- Avoid Eating while using the device
- Avoid hard pressing the keyboard keys and mice buttons
- Always Scan Portable Storage devices from viruses
- Regularly clean from dust

Electrical Power boards and Lead wires

- Avoid plugging high wattage appliances – use permanent power point wall outlet instead.
- Avoid Exceeding maximum rate.
- Place it in a convenient place for easy access and safely and free from busy workspace and out of the way from walking paths to avoid cable entanglement.
- Avoid Liquids and Food crumbs and stains on the Power board and Lead wires

ANNEX D: Minimum Hardware Specifications

KAO ICT Assets and System Requirements:

Below are listings of all the ICT equipment/devices that are required for the Kiribati Audit Office to enable its staff to carry out their Auditing and/or daily work-related activities effectively and efficiently. The KAO Office may not be able to carry out its tasks without at least meeting the minimum requirements of the items mentioned below.

1. COMPUTERS: (42 users) + SERVER(S)

Computers are essential part of the workplace for staff to perform variety of tasks especially the use of Microsoft office products, working with databases and accounting packages, accessing the Local Network and Internet, etcetera.

Types of Computers with their use, assignment, and specification requirement.

1.1 LAPTOP: (35 USERS)

All Auditors due to the nature of their work, are entitled to a laptop with the minimum specifications provided below which will be sufficient to perform required daily/auditing tasks. Non-Auditors may temporarily acquire a laptop (spare) with the approval of the SRO.

Laptop minimum requirements:

- Windows 10 Pro (Operating System)
- Core i3 CPU
- 4GB Ram
- 15.6-inch Screen
- Numeric Keypad
- Good users' rating/reviews
- USB mouse & keyboard (optional)
- 19inch monitor (optional)
- Laptop bag

Junior Staff Laptop should meet the minimum requirement, but if the specification of a laptop to be bought is higher than the minimum but cheaper, it will be considered as a preferable choice. HOD Staff should always have higher CPU and RAM specifications than the minimum requirement.

1.2 DESKTOP: (5 USERS)

Non auditors like the administration staff (except for drivers and cleaners) are entitled to a Desktop computer with the following required minimum specifications:

Desktop minimum requirements:

- Form-Factor Mini-Desktop
- Windows 10 Pro (Operating System)
- Core i3 CPU
- 4GB Ram
- Built-in Wi-Fi adaptor
- Good users' rating/reviews
- 19inch Monitor

1.3 WORKSTATION: (2 USERS ICT SPECIALIST)

A workstation is a much more powerful Desktop/Laptop which is mainly used for running resource demanding applications, tests in a Virtual Environment, Graphical intense programs for designing and Developments etc. This workstation is entitled to an ICT Specialist for the above-mentioned purposes.

Workstation recommended specification:

- Windows 10 Pro (Operating System)
- Core i7 CPU
- 8GB Ram
- GTX 1050 GPU (Video Card) or AMD similar
- SSD OS Drive
- 4TB HDD Storage Drive
- 22-inch Monitor

1.4 SERVER: (ICT ADMINISTRATORS)

The Server Computer provide network services and resources (such as file sharing, hosting network programs, etc…) to network users and devices. This server should be managed by ICT Staff only.

Server recommended requirement:

- Server 2016
- CPU: Intel Xeon or AMD Epyc or AMD Threadripper
- 16GB Ram
- 250GB SSD OS Drive
- X2 4TB HDD Storage Drive
- UPS 2000VA
- 19inch monitor
- USB Mouse and Keyboard (Optional)

2. NETWORK DEVICES:

Network devices are physical devices which are required for communication and interaction between devices or users on a computer local/wide area network. These Network devices will be managed and monitored by ICT Staff. Below you will find all network devices that are required by KAO with their use and required specifications.

Types of Network devices with their use and specification requirement.

1.4 FIREWALL (HARDWARE OR SOFTWARE)

A Firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined KAO network security rules. It could be software based, network device or a computer configured as a firewall.

Firewall features requirements:

- Filter websites
- Support active directory
- Access/Time scheduling

- Data and Bandwidth management
- Manage, monitor users' usage.
- Caching

2.2 GATEWAY (INTERNET)

A gateway is a hardware device that acts as a "gate" between two networks (Office Network and Internet). It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.

This device is normally provided by the Internet Service Provider (ISP) or can be any device mentioned above with the configuration of the ISP's setting.

Internet Gateway only requires that the internet speed is fast (100Mbps or more), and it is reliable.

2.2 WI-FI ROUTER

Wi-Fi Router is a network device that allows Wireless, or Ethernet connected devices such as Computers, printers, smartphones etc... to connect and access Resources Shared on the Network or access Internet.

Wi-Fi Router recommended requirements:

- Omni directional antenna
- Tri-band frequency
- WPA2 Security
- Gbps speed
- 802.11ac standard
- DHCP service

2.4 POINT TO POINT WIRELESS OUTDOOR BRIDGE X2

These network devices are used to connect KAO separate office buildings wirelessly or nearby outdoor users. These devices are normally mounted outdoors, raised, and positioned in line (clear line of sight) with each other for stability connection.

Recommended requirements:

- 802.11ac standard
- Gbps speed
- WPA2 Security
- Weatherproof

2.5 FINGERPRINT PUNCH ATTENDANCE DEVICE

A device (connected to the Network) which records the attendance of all KAO Staff by reading each staff unique fingerprint and store it on its own Software (installed on Server) for reporting.

2.5 ONLINE VIDEO CONFERENCING EQUIPMENT

These devices will allow staff to do video calls online as individuals or as a group to join meetings, trainings, workshops, etc. virtually. The minimum requirement are as follows:

- External Webcam: Must be able to capture everyone in the conference room with a clear picture quality.
- Speakerphone: Must be able to capture/record audio everyone in the conference room.
- TV Screen: Must be big enough to be seen by everyone in the conference room with excellent picture quality.

2.7 MULTIFUNCTION INKJET PRINTER FOR EXECUTIVES

Inkjet printers are the most used type of printer. It uses ink cartridges by recreating a digital image by propelling droplets of ink onto paper. Since it is slower than Laser Printers, multiple print jobs from different sources might queue up the printing very quickly. Therefore, this type of printer is entitled to executive staff only.

Inkjet Printer requirement:

- Colour
- Multifunction (Print/Scan/Copy/Fax)
- Wireless or Ethernet
- Duplex

2.8 MULTIFUNCTION LASER PRINTER (COLOR) FOR STAFF

The Office should have a Multifunction Laser Printer for fast printing, scanning, and copying to avoid multiple print jobs queue delays. This printer should be managed by ICT Staff to avoid staff misuse of the printer.

Laser Printer requirement:

- Colour
- Multifunction (Print/Scan/Copy/Fax)
- Wireless or Ethernet
- Duplex
- 30000 pages per month
- Affordable/Reliable Toner(s)

2.9 SURVEILLANCE CAMERA

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, maintained, and monitored by ICT Staff. This is useful in preventing or solving issues like theft, liability claims, safety, etcetera.

Surveillance Camera minimum requirement:

- 4 Channels
- 4TB Storage (16TB Recommended)
- Network Video Recorder (NVR)
- Night vision
- 1080p resolution
- Outdoor support

2.10 BACKUP STORAGE (OFFSITE):

Although the Server Computer has its own backup storage drive, an Offsite backup is a method of computer data backup involving the use of an offsite location as a means of securing in the event of a disaster. This Offsite backup storage will be a backup of the Server's backup storage (backup of a backup).

Offsite Backup storage requirement:

- 4TB HDD
- Network Attached Storage (NAS)
- Rugged/Waterproof/Fireproof

3 OTHER TOOLS, DEVICES AND NECESSITIES:

Other ICT necessities that are required by KAO. Most of the items below are managed by ICT Staff unless they are specifically assigned to any individual staff with the approval of SRO.

3.1 PROJECTOR

A projector is an optical device that projects an image (or moving images) onto a surface, commonly a projection screen. Occasionally KAO staff is required to communicate the content, purpose, and value of the work to an audience (e.g., Presentations). Projectors help that communication by expanding the image of your computer screen to be large enough for an audience to see.

Projector minimum requirements:

- 1080p resolution
- HDMI port
- DLP or LCD

3.2 MOBILE SMARTPHONES (ON CALL USERS)

KAO Should provide mobile phones for on call staff. These staff should always be available via phone calls or online call/message when they are needed: These staff are usually drivers for their transport services and cleaners who holds the key to the office. Additional staff may also have this entitlement if necessary.

No specific requirement is needed for a smartphone, a basic smartphone with a 4G LTE capability is good enough for the purpose mentioned above.

3.3 SERVER CABINET

A Server Cabinet is used to house and organize ICT equipment in a manner that is best for the optimization of the equipment and utilization of floor space. The Server Cabinet usually contain its own power source with surge protection, and it is well ventilated. KAO requires this Cabinet to house its Computer Server with its UPS and maybe some Network devices.

3.4 STORAGE CABINET OR SHELF (FURNITURE)

Storage cabinets are very useful for offices as they allow users to store and maintain their files, documents, devices, and equipment appropriately. ICT Staff require this Storage Cabinet for the same reason as mentioned.

3.5 ETHERNET CABLE ROLL

Almost all network devices are connected via Ethernet cable if they are not connected wirelessly. This cable must always be available to the ICT Staff in case some older cables might need replacement or new connection may be needed.

3.6 PC & NETWORK TOOLKIT

All the devices mentioned above may require maintenance and repair. ICT Staff should have a complete set of proper tools to maintain the usability of all the above-mentioned devices.

A complete set of tools should have the followings:

- Flat-head screwdriver (Set)
- Phillips-head screwdriver (Set)
- Torx screwdriver/wrench (Set)
- Hex driver (Set)
- Adjustable Shifter/Wrench
- Crimping Tool (RJ45)
- Digital Multimeter
- Dust Brush
- Air Blower/Compressed Air
- Anti-Static wrist strap/Mat
- Toner Probe
- Cable Ties
- Tweezers
- Parts Organizer
- Small flashlight
- Soft, lint-free cloth
- Scissors
- Electrical tape
- Work-space Table

ANNEX E: Computer Fresh Install & Maintenance Procedure

Instructions for ICT Staff only on how to proceed with a fresh install of Windows 10 Professional or Reset/Upgrade Install of an Operating System (Maintenance) on KAO Computers.

- FRESH INSTALL for new Computers

    - Create a UEFI Bootable Windows 10 (Latest Update) USB drive.
    - Install Windows 10 on Computer (UEFI boot on USB Drive)
    - Create separate Hard Drive Partition called Storage and Install OS on other partition.
    - Disable all updates/auto-connect to internet features during OS install.
    - Set Country (Region): Kiribati, Language: English (International), Keyboard Layout: English (US).
    - Create Local Administrator: KAO ITAdmin as username and password: k**@******t**_*****v

- RESET / UPGRADE WINDOWS 10/11 during Maintenance

- CONFIGURATIONS AFTER WIN10PRO INSTALLATION/RESET:

    - Correct date and time (manually)
    - Activate Windows
    - Rename computer to whoever is going to use the computer in the format e.g. KAO-NAME (restart).
    - Connect to KAO Wi-Fi
    - Enable/Allow Remote Connection
    - Connect to \\kao-dc-01 Server using the Admin credentials
    - Copy KAO software requirements from \\kao-dc01\Resources\KAO ICT\Software to Computer's Storage Drive.

- KAO SOFTWARE INSTALLATION:

    - Give device direct access to Internet
    - Install ALL Windows Update
    - Install NetFramework 3.5 using Win10 image (mounted) and running batch script provided as Administrator
    - Install Laptop Genuine drivers only (download online) otherwise use DriverPack (check Readme instruction)
    - Install 7Zip (update it)
    - Install Microsoft 365
    - FileMaker 18 (check Readme instruction)
    - Adobe PDF Reader make it default reader (don't make a shortcut icon), update it.
    - Wordweb Dictionary (check Readme instruction) and update it.
    - VLC Player (check Readme instruction) and update it.
    - Install MYOB (only required versions)
    - Put Proxy script in C:/windows
    - Install Achat
    - Install Firefox Browser (update to the latest version)

- Disable unnecessary auto-startup apps except (Defender, WordWeb, Achat)
- Complete Windows Defender Antivirus setup and update it.
- Restart (Computer Setup DONE… now ready for User setup)

- CREATE STAFF LOCAL USER ACCOUNT: in the format: username as Full Name, and password: by following password crypto text guide kept privately by ICT Department.

  - Login to the newly created User Account
  - Set these desktop icons only: This PC, Recycle Bin, Filemaker, Firefox, VLC, WordWeb). Remove the rest.
  - Set default apps to Firefox, 7Zip, VLC, Adobe Reader.
  - Run VLC and untick update and network options
  - Run Achat and set option to auto-startup with windows and disable popup bubbles
  - Map the necessary Network Drives using user credentials
    - Junior Staff: *Shared, Resources, Scans, Social Committee, Section, Work Folder*
    - Senior Staff: *Shared, Resources, Scans, Social Committee, Section, Staff Folder, HOD*
    - HOD Staff: *Shared, Resources, Scans, Social Committee, concerning Sections, Staff Folder, HOD.*
    - Registry Staff: *Shared, Resources, Scans, Social Committee, Section, Database, Staff Folder.*
    - IT Staff: *ALL, except other Staff Folders.*
    - Training: *To staff attending a Training.*
  - Add and Configure Network Printers and run test a test print.
  - Remove unwanted Taskbar icons and replace with only; Search Icon, This PC, Filemaker, VLC, Firefox, Word, Excel
  - Remove all Start Menu Tiles and Add only; This PC, Filemaker, VLC, Firefox, Word, Excel, Calculator, wordweb.
  - Configure taskbar to Combine taskbar buttons “When taskbar is full”.
  - Sign In to Office365 and update it.
  - Configure Filemaker Database to join Server database (add from Host)
  - Create a bookmark login page on Firefox for the official email.
  - Configure Internet Proxy in the Control panel (file://c:/windows/proxy.pac), Reserve IP in DHCP Server and Update the CCProxy.
  - Restart (Computer Setup for User is COPMLETED)

- FILL AND HAVE THE USER SIGN THE LAPTOP LENDING AGREEMENT OR THE MAINTENANCE LOG
- UPDATE ITEM POSSESSION RECORD ON DATABASE IF COMPUTER IS NEW OR BEING TRANSFERRED.
- BOOK ITS NEXT MAINTENANCE SCHEDULE
- DONE.

ANNEX F: KAO Software

Below is a list of approved Computer Software for the Kiribati Audit Office. The listed software must be updated frequently to the latest version and must have genuine license.

All Staff Computer Software

- Office 365 package
- Filemaker Pro
- Adobe Acrobat Reader
- Firefox Internet Browser
- 7zip
- Wordweb dictionary
- VLC Player
- Zoom
- Achat

Extra Software for Audit Staff

- MYOB

Auditor General extra software

- Network Video Camera Software

ICT Staff Computers

- Since ICT Staff have the right to install and uninstall a software, they may have all the software listed above plus extra software not listed here for testing purposes.

Server Software

- Filemaker Server
- FBackup
- Fingerprint Attendance Software (Fingertech)
- CCProxy Firewall (Software)
- Teamviewer
- OpenVPN
- ABC UPS Netguard

ANNEX G: Computer Maintenance Schedule

All KAO Computers are expected to go through maintenance on an annual basis to improve the lifespan. The maintenance process is complete when both the concerning staff and the maintenance officer sign the sheet below. Both should make sure that all necessary steps in Annex E are done in the process.

Below is a schedule for maintenance on user's computers.

Staff Name	**Computer/Model**	**Schedule Date**	**Maintenance by: ICT Officer**	**Maintenance Completed: ICT Signature**	**Confirmation by: Staff Signature**

ANNEX H: Computers & ICT Devices Lifespan

This policy provides guidelines regarding the life span and refresh rate of KAO ICT Computers and Devices. The lifespan is the period during which the ICT equipment remains useful, while the refresh rate is the planned rate of replacing such equipment. The objective of this policy is to establish and define a Refresh policy for all ICT equipment used in the KAO. This is intended to provide a balance between optimum use and on-going maintenance costs to enable staff to use the latest software with ease, without impeding the productivity and efficiency of the agencies with the Government.

The purpose of this policy is to minimise risk(s) from (but not limited to):

- Vulnerability of out-date or obsolete hardware and software systems to external and internal attacks
- In-adequate security and authentication functions for obsolete systems
- Unavailability of Security fixes and vulnerability patches for obsolete systems.
- The lack of technical support and defensive measures available to obsolete systems.

This policy applies to all KAO owned and leased ICT equipment used by the KAO and its Staff (As listed in Table A).

ICT Equipment Refresh Policy:

1. ICT equipment will be refreshed in which they are determined to be obsolete or end-of-life (operating beyond its determined Life Span) or when deemed non-functional by the Office.
2. ICT Equipment or accessories stolen or lost will be reported to the relevant authorities and will be replaced only at the discretion of the Auditor General or appointed representative.
3. ICT Equipment having minor wear and tear within the stipulated lifecycle, and is still deemed functional by the ICT Staff, will not be refreshed, or replaced.
4. All ICT equipment will have the Life Span and Refresh rate as proposed in Table A.
5. This policy and the content of Table A will be reviewed as deemed appropriate, but no less frequently than every 12 months.

Table A. ICT Equipment Lifespan and Refresh Rate.

Equipment Type	Life Cycle (in years)	Refresh Rate (in years)
Laptop Computer	5	3
Mini Desktop Computer	5	3
Computer Monitor	8	6
Server Computer	5	4
Multipurpose Laser Printer	7	5
Multipurpose Inkjet Printer	7	5
Single Purpose Laser Printer	7	5
Wireless Router	5	5
Network Switch	5	5
TV Screen	7	7
Conference Webcam	5	5
Conference Speakerphone	5	5
Network Video Recorder	4	4
Fingertech Attendance Machine	7	7

ICT Devices not listed in the table will be replaced if lost or damaged.

ANNEX I: Staff Laptop Assignment

1. Introduction

This policy outlines the procedures and guidelines for the assignment, maintenance, and replacement of laptops provided to staff. It aims to ensure that all staff have the necessary tools to perform their duties efficiently while maintaining accountability and proper care of company assets.

2. Categories of Laptops

Laptops are categorized into four types:

1. New Laptops: Brand new laptops assigned to permanent staff.
2. Used Working Laptops: Previously used laptops that are still functional.
3. Used Broken Fixable Laptops: Laptops that are broken but can be repaired.
4. Used Broken Unfixable Laptops: Laptops that are beyond repair and are used for spare parts or disposed of.

3. Assignment Rules

New Laptops:

- **Eligibility**: New permanent staff should be assigned a brand-new laptop.
- **Replacement Cycle**: Laptops should be written off and replaced every three years, can be extended to no later than 5 years.
- **Condition for Replacement**: A staff member should not receive a brand-new laptop until their current laptop is written off, unless there is a compelling reason requiring a new laptop.
- **Priority**: New laptops should be given first to those who have maintained their current laptops to standard, and then to those who did not take proper care of their laptops.
- **Record Keeping**: All new laptops must be properly recorded in the Office database.

Used Working Laptops:

- **Temporary Staff**: Used working Laptops should be assigned to temporary staff.
- **Staff with Repaired Laptops**: Used working laptops should be temporarily assigned to staff whose current laptops are undergoing lengthy repairs.
- **Staff with Damaged Laptops**: Used working Laptops should be assigned to staff who have broken their new laptops beyond repair. These staff members will use a used working laptop until the write-off cycle of the broken laptop (three years) is complete, at which point they will be eligible for a brand-new laptop.

Used Broken Fixable Laptops:

- **Repair and Reassignment**: These laptops will be repaired by ICT and will under the “Used Working Laptops” category.

Used Broken Unfixable Laptops:

- **Spare Parts**: These laptops should be utilized as a source of spare parts to prevent work downtime.
- **Disposal**: Unfixable laptops will be disposed of properly according to the e-waste disposal act.

Important related topics: refer to Annex A,B,C of the KAO ICT Security Policy 2023.