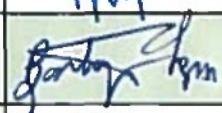




KMNYA PLANT HEALTH INSPECTORATE SERVICE

ICT POLICY

DOCUMENT CONTROL

	NAME AND TITLE	SIGNATURE	DATE
Author			27/5/2020
Approved	Head - ICT		27/5/2020
Release Authority	GN- Finance and Administration		28/5/2020
	managing Director		
Maintenance Distribution	ICT Department		
	This document will be published on the KEPHIS's website for controlled and Authenticated downloads. Copies can be availed for download via staff email		

REVISION DETAILS

REVISION NUMBER	REVISION SUMMARY	REVISED BY	SIGNATURE	DATE
D01	Review of the whole document to ensure compliance to ISO/IEC 27001 standard guidelines	Head ICT		27/5/2020

TABLE OF CONTENTS

1.0	Preamble	3
1.0	Scope	4
3.0	User Access Policy	5
	External Parties	6
5.0	Data Backup Policy	6
6.0	Internet, E-Mail, and Computer Use Policy	6
7.0	Policy on Passwords.....	8
8.0	Data Center/Server Room Policy.	8
9.0	ICT Software Policy	10
10.0	System Development Acquisition and Maintenance.....	11
11.0	ICT Removable Media Policy	11
12.0	Policy on ICT Technical Support Request and Complaints.....	12
13.0	Mobile Devices (Tablets and Mobile Phones Policy).....	12
14.0	Disposal of Old Equipment.....	2
15.0	Email Retention	13
16.0	Bring Your Own Device Policy	13
17.0	Clear Desk Clear Screen Policy.....	14
18.0	Teleworking Policy	16
19.0	Business Continuity Management Policy	16
20.0	Policy on Printers, Telephone Lines, and Copiers.....	16
21.0	Review of the ICT Policy	17

1.0 Preamble

- 1.1. The purpose of this Policy is to ensure that all use of KEPHIS Information, Communications and Technology (ICT) systems is legal, ethical and consistent with the Vision, Mission and Strategic plan of KEPHIS. It is a suite of safeguards, guidelines and procedures intended to protect, build confidence both among staff and external parties by ensuring the preservation of confidentiality, integrity and availability of information resources.
- 1.2. This policy promotes the responsible use of information resources in line with accepted international standard ISO/IEC 27001 framework for information security. The loss or corruption of data or unauthorized disclosure of information could greatly hinder the legitimate activities of KEPHIS. KEPHIS has an obligation to ensure security of its resources including computers and associated networks.
- 1.3. KEPHIS ICT systems shall be properly and efficiently used while ensuring security of the information as well the systems. KEPHIS ICT systems are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, sexual harassment, stalking, privacy violations or any other illegal activity.
- 1.4. This ICT policy is neither exhaustive nor exclusive. It is meant to complement and support other related KEPHIS policies that include among others: The KEPHIS E-Waste Policy and the KEPHIS HR Manual and guidelines.
- 1.5. It is the responsibility of General Managers, Heads of Departments and Section Heads to ensure that the persons to whom this Policy applies are aware of this Policy. This shall include, but is not limited to: providing access to a copy of the Policy; reminders of the need for compliance with the Policy; and providing updates or developments of the Policy, to those affected by the Policy.
- 1.6. It is the responsibility of all ICT System users to abide by this Policy.
- 1.7. Non-compliance with this Policy will be regarded as a serious offence and shall lead to a disciplinary action or report to the police if the breach is deemed to be also criminal as per the laws of the Republic of Kenya.

2.0 Scope

In this Policy —

- 2.1. An "Authorized Person" means an individual who is formally and properly empowered to perform specified duties associated with an office or an agreement or contract.
- 2.2. "KEPHIS" means the KENYA PLANT HEALTH INSPECTORATE SERVICE.
- 2.3. "KEPHIS ICT systems" includes but is not limited to, email system, Information Systems and databases, operating systems (windows and Unix/linux) ,LAN ,WAN internet, telephone systems, wireless communication, printers ,copiers., servers, desktop computers, notebook computers, mobile phones, digital cameras, photocopying machines, hand held devices (for example, personal digital assistants or "PDAs"), USB memory sticks and other ICT storage devices;
- 2.4. "Electronic communications" The term electronic communication is defined as passing of information from one individual to another using computers, fax and phones. A good example of a form of electronic communication is the use of email;
- 2.5. "Personal use" means all non-work related use, and includes non-work internet usage and private emails.
- 2.6. "Users" of KEPHIS ICT systems includes all employees (including ongoing, temporary employees) and contractors engaged by KEPHIS and authorized to use the information systems.
- 2.7. This Policy applies to all users of KEPHIS ICT systems regardless of work location.

2.8. This Policy applies to the use of all aspects of KEPHIS ICT systems, networks, software and hardware collectively referred to as "KEPHIS ICT systems".

2.9. Use of KEPHIS ICT systems includes transmissions to or through KEPHIS ICT systems by a user.

3.0 User Access Policy

3.1. Request for System Access by New Users

- 1. Departmental support staff shall request an account through their supervisor or departmental head. The legitimacy of each request will be evaluated and, if approved, the user will be assigned a specific level of security clearance.**
- 2. An employee shall request access for his/herself; however each access request shall be approved by a Supervisor or Department Head.**

3.2. Process for Granting or Declining Requests

1. When a request is submitted, the user is prompted to provide the ID(s) and shall sign off on the KEPHIS Administrative Security form. The request shall be made through the form available online or via the ICT Service Desk System.
2. The approver has the option to "Approve" or "Deny" the Access Request. If an Access Request is denied the approver shall supply a comment as to why they are denying the Access Request.

3.3. Request for Modified User Access

1. modification of access rights on the system shall be granted once the user requests through KEPHIS Administrative Security form.
2. The current access rights and the new /requested rights shall be included on the modified form.
3. The respective system administrator shall ensure that upon granting new access rights, the previous access rights are revoked.
4. A Confidentiality or non-Disclosure Agreement reflecting organization's needs for protection of information shall be signed by all staff.

4.0 External Parties

The risks to the organizations information and information processing facilities from business processing involving external parties shall be identified and addressed before granting access to the organizations information or assets. Appropriate contacts with relevant authorities, special interest groups and other specialists' security forums and professional associations shall be maintained.

5.0 Data Backup Policy

KEPHIS will ensure the following about the backup system.

- 5.1. The organization's data shall be backed up every day or as frequently as deemed fit by the organization.
- 5.2. ALL important information shall be backed up; this shall include data in Information systems as well as shared folders on the network. A schedule of all the data being backed up will be maintained at all times.
- 5.3. Users shall save all their working documents on a shared folder on the network which shall be backed up periodically. All data not saved in the shared folders will not be backed up and will be the responsibility of the user.
- 5.4. The backed up data/information will be restored and tested periodically ensuring that it is usable in the event of data loss.
- 5.5. A copy of the backup will be kept at an offsite location at all times.

6.0 Internet, E-Mail, and Computer Use Policy

KEPHIS has established the following policy guidelines for employee use of the company's technology and communications networks, including the Internet and e-mail, in an appropriate, ethical and professional manner.

- 6.1. All technology provided by KEPHIS, including computer systems, communications
- 6.2. Networks, company-related work records and other information stored electronically in the systems, is the property of the company and not the employee.
- 6.3. Use of the company's technology systems and electronic communications shall be work-related and not for personal use.

- 6.4. Users will not use KEPHIS's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature.
- 6.5. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted through KEPHIS electronic communications system. Harassment of any kind is prohibited.
- 6.6. Disparaging, abusive, profane or offensive language; materials that might adversely or negatively reflect on KEPHIS or be contrary to its legitimate business interests; and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail are forbidden.
- 6.7. Copyrighted materials belonging to entities other than KEPHIS shall not be transmitted by employees on the company's network without permission of the copyright holder. Employees shall respect all copyrights and shall not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only.
- 6.8. Saving copyright-protected information to a network drive without permission is prohibited. Sharing the URL (uniform resource locator or "address" of an Internet site with other interested persons for business reasons is permitted. Users shall not use the system in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and "spamming" (sending e-mail to thousands of users.)
- 6.9. To prevent contamination of KEPHIS technology and communications equipment and systems by harmful computer viruses, downloaded files shall be scanned by the antivirus. Also, given that many browser add-on packages (called "plug-ins") shall not be compatible with other programs and shall cause problems for the systems, downloading plug-ins shall be monitored by IT.
- 6.10. Every user is responsible for the content of all text, audio or image files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications shall be sent that hide the identity of the sender or represent the sender as someone else. KEPHIS's corporate identity is attached to all outgoing e-mail communications, which shall reflect corporate values and appropriate workplace language and conduct.
- 6.11. Users shall only send Email to those meant for; and avoid broadcasting (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer and network performance and wastes disc space and shall not be allowed.

- 6.12. Users shall not broadcast emails with attachments to large groups of people - Users are expected to use efficient means of sharing of files that shall include link to a cloud/server storage. Failure to do this puts an unnecessary load on the network.

7.0 Policy on Passwords

The following policy guidelines will guide the use of passwords in all KEPHIS Systems including domain, e-mail and business application accounts:

- 7.1. User shall not disclose the password to anyone.
- 7.2. Shall be a combination of alphanumeric and special characters (! ? \$ ^ % & #), i.e. Complex, but easy to remember.
- 7.3. Passwords shall be at least eight (8) characters.
- 7.4. Users are required to change their passwords at least every 60 days
- 7.5. Passwords shall lock for repeated unsuccessful attempts. Account lockout of d invalid login attempts shall be enforced on the Information systems. Idle session timeout of up to a maximum of 6 minutes shall be enforced on information systems. Password History of up to 5 shall be enforced. This is to ensure that users do not repeat their passwords once prompted to change.
- 7.6. Password Management will be the responsibility of the Systems Administrators.
- 7.7. A user whose password has expired, or account locked shall (upon request through IT support) be assigned an initial password by the systems administrator. The affected user shall change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.

8.0 Data Center/Server Room Policy.

7.1. Access Policies and Procedures - Individuals

- IT Staff: I.T staff whose job descriptions directly relate to the management of the Data Center or the shared resources contained therein shall be granted access to the KEPHIS server room facilities.
- Vendors, Contractors, and Other Visitors: Vendors, contractors, and other visitors shall gain access to KEPHIS server room facilities upon registration with the

I.T DEPARTMENT and with the authorization of an approved sponsor or an escort.

Approved sponsors are those individuals who have key access to the space.

- **Access Privileges: Failure to comply with this policy shall result in revocation of access to all IT managed facilities and appropriate staff disciplinary action.**

7.2 Access Policies and Procedures - Computing Devices

- **Registration:** Computing devices capable of communicating with other devices via standard protocols (including, but not limited to TCP/IP) shall be registered and approved prior to being allowed in any of the KEPHIS server room facilities or connected to the organization's network.
- **KEPHIS Computing Devices:** KEPHIS computing devices shall be in the possession of a KEPHIS staff member who is pre-authorized for data center/server room entry for it to be admitted into the server room. Only KEPHIS-acquired computing devices are allowed in any of the KEPHIS server room facilities. Personally-acquired or owned, non-KEPHIS computing devices are not allowed in the facilities.
- **Vendors and Service Contractors Computing Devices:** Vendor and service contractor computer device registrations shall be granted by the ICT department. At no time are these devices to be plugged into a data center network port (such as a network switch) or to utilize wireless communications (other than cellular telephone services) without prior approval from the ICT department.

7.3. Custodial Responsibilities for the IT Data Center

- Rules and guidelines for conduct within the KEPHIS Data Centers/Server room facilities are designed to safeguard the equipment within the facility, the staff and users of the facility, and the shared activities served by the facility. All users of the facility are asked to observe these custodial responsibilities as outlined below.
- **Climate:** Climate conditions in the Data Center will be continuously monitored by the I.T DEPARTMENT staff and adjusted as needed for optimal results. Individuals who are not members of the I.T DEPARTMENT staff shall not adjust the settings on any HVAC units as they affect all users of the shared data center. Notify the I.T DEPARTMENT if climate conditions are sub-optimal for the computing environment. The I.T DEPARTMENT will coordinate regularly scheduled preventative maintenance on the HVAC units.
- **Cabling:** All cables are to be labeled at both ends designating the location and system identifier. Cables shall be contained within the equipment rack and not extend into the aisle. All inter-rack cabling shall be through cable trays or designated paths under the raised floor tiles.

9.0 ICT Software Policy

- 9.1. Only software and digital media authorized or supplied by the ICT Department shall be installed on KEPHIS owned equipment. Usage of all software and digital media shall be in compliance with the terms and conditions of the associated license agreements.
- 9.2. Software or digital media will only be installed on KEPHIS equipment where evidence of the purchase of adequate licenses can be demonstrated to the ICT Department.
- 9.3. All media, documentation and license certificates will be retained by the ICT Department.
- 9.4. Software Installation and Removal shall abide to the following policy guidelines:
 - a) Only ICT Department staff, or individuals authorized to do so by the Head of ICT shall install, load or copy software or digital media onto KEPHIS owned ICT equipment.
 - b) Prior to installation, confirmation shall be made by the individual installing the software that a valid license exists. It shall be ensured that the license agreement permits use of the software for the purposes for which it is being installed;
 - c) Individual installing the software shall ensure that: Software licensed for testing purposes, for example, beta versions, is not used in a "live" environment and also that the installation or removal of software or digital media from any ICT hardware shall be reflected in the Software Asset and License register. Updates shall be carried out within a period of 7 working days, either through an automated process or a manual adjustment.
- 9.5. In-house software: This is software written by staff or volunteers using KEPHIS equipment. In-house software shall be a KEPHIS property and shall not be used for any external purpose. Software developers employed at KEPHIS are permitted to take a small "portfolio" of such in-house software source code/executables, which they shall have developed, for use in subsequent work, subject to agreement with the Head of ICT.
- 9.6. The transfer of Original Equipment Manufacturer (OEM) supplied software to another device is not permissible under any point.

10.0 System Development Acquisition and Maintenance

- 10.1. The information security related requirements shall be included in the requirements for new information systems or enhancement to existing information systems.
- 10.2. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification
- 10.3. Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized message duplication or replay.
- 10.4. Rules for the development of software and systems shall be established and applied to developments within KEPHIS
- 10.5. Changes to systems within the development lifecycle shall be controlled by use of formal change control procedure
- 10.6. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security
- 10.7. Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
- 10.8. KEPHIS shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. The organization shall supervise and monitor the activity of outsourced system development
- 10.9. Testing of security functionality shall be carried out during development. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. Test data shall be protected and controlled.

11.0 ICT Removable Media Policy

- 11.1. Removable media shall be kept safely: In order to minimize storage risk, loss, theft or electrical corruption, all storage media containing KEPHIS business information shall be stored in an appropriately secure and safe environment.
- 11.2. **Virus and malware checking:** Virus and malware checking software approved by the ICT Department shall be operational on both the machine from which the data is taken and the device onto which the data is to be loaded. The data shall be scanned by the KEPHIS Antivirus software before the media is loaded on to the receiving machine.
- 11.3. **Disposing of removable** media devices: Removable media devices that are no longer required, or have become damaged, shall be disposed off securely. Any previous contents of any reusable media that are to be reused, either within the

KEPHIS or for personal use, shall be sanitized appropriately. All removable media devices that are no longer required, or have become damaged, shall be returned to the ICT Department for secure disposal.

12.0 Policy on ICT Technical Support Request and Complaints

- a) All ICT requests for technical support shall be channeled through the centralized ICT Help Desk System or by calling the ICT helpdesk line.

13.0 Mobile Devices (Tablets and Mobile Phones Policy)

The following policy guidelines will guide the use of Mobile devices on the KEPHIS systems and within KEPHIS:

- 13.1. Each user shall ensure duty of care whilst using such devices to ensure that they are used for their intended purpose only, without creating business risks, by understanding the way the mobile devices shall be used.
- 13.2. All KEPHIS supplied tablets, phones or any other mobile device shall be the property of KEPHIS and can be audited and monitored, similar to any other electronic device.
- 13.3. Users shall take reasonable care to protect the device from loss or theft.
- 13.4. Users shall immediately inform the ICT Department and their respective heads when the device is stolen or lost.
- 13.5. In the event that a KEPHIS tablet or phone is lost or stolen, the service provider shall be informed immediately to block the SIM card.
- 13.6. The installation of unauthorized third party software shall not be supported by ICT and shall be uninstalled when immediately discovered.
- 13.7. Network and system passwords shall not be stored on mobile devices.
- 13.8. Users shall report any fault with the device to IT department in the first instance. If the device fails and needs repair or restoration, The ICT Department shall restore the device to the state it was in on first delivery to the user.
- 13.9. KEPHIS owned portable mobile devices no longer required shall be returned to the ICT Department for the device to be redistributed.

14.0 Disposal of Old Equipment

The frequently changing IT environment means that computing equipment (personal computers, laptops and peripherals such as printers) periodically becomes surplus to requirements or reaches the end of its useful life. The disposal of obsolete ICT equipment shall be guided by the KEPHIS E-Waste Policy.

15.0 Email Retention

- 15.1. This email retention policy is secondary to the Kenya Freedom of Information Act/or any other relevant government legislation. Any email correspondence containing KEPHIS information will therefore be retained through backups or any other means as deemed needed.
- 15.2. The organization shall retain all company mails for a period of 1(one) year after which the mails shall be deleted. It is the responsibility of the users to archive their mails which are more than one year if necessary.
- 15.3. The primary intent of email backup is for the full recovery of the current and previous email system .The ICT Department will back up the email system solely for the purpose of restoring the service when it suffers a catastrophic system failure and the whole system has to be restored.
- 15.4. The ICT Department shall set the parameters for users' storage space and email archiving solution that would among other things set the limit of e-mail stored in the server, and enable users to archive their own emails.

This policy establishes guidelines for employee use of personally owned electronic devices for work-related purposes. It is intended to establish rules for employee behavior necessary to protect the privacy, security and integrity of KEPHIS's data and technology infrastructure against the risks that can arise when employees use their personally owned devices for business purposes

Policy Guideline

A. General Principles Users shall:

Use of personal devices for KEPHIS work shall be approved by the relevant business heads and the Head of ICT.

- i. **Use the device security features, such as a PIN, Password/Passphrase and automatic lock to help protect the device when not in use.**
- ii. Keep the device software up to date, for example using Windows Update or Software Update services.
- iii. **Activate and use encryption services and anti-virus protection if applicable**
- iv..

V. Remove any KEPHIS's information stored on the device after use including deleting copies of attachments to emails, such as documents, spread sheets and data sets

VI. Limit the number of emails and other information synced to the device to the minimum required.

vii. Remove all KEPHIS's information from the device and return it to the manufacturers' settings before selling, exchanging or disposing it

B. Acceptable Use policy guideline (Clause.) shall apply for all approved personal devices used within KEPHIS and/or for KEPHIS work.

ii. The company reserves the right to disconnect devices or disable services without notification.

iii. Lost or stolen approved personal devices shall be reported to KEPHIS within 24 hours for the purposes of mitigating information security risks. Owners of the devices are responsible for notifying their mobile carrier immediately upon loss of a device.

V. The employee is personally liable for all costs associated with his or her device.

VI. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable

17.0 Clear Desk Clear Screen Policy

The objective for this policy is to establish a culture of security and trust for all employees at KEPHIS. An effective Clear Desk and Clear Screen effort involving the participation and support of all KEPHIS employees can greatly protect all documents that contain sensitive information about our clients, customers and vendors. It applies to:

- i. All KEPHIS staff, partners, suppliers and contractors with respect to KEPHIS information assets;
- ii. Employees, representatives and agents from other organizations who directly or indirectly support **KEPHIS** information systems, including auditors and other external consultants;
- iii. All KEPHIS information assets and information processing facilities without exception;

Policy Statement

i. Clear Desk

Where practically possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office /room doors shall be locked if left unattended. At the end of each session all sensitive information shall be removed from the work place and stored in a locked area. This includes all business-critical information such as salaries and contracts.

Confidential sensitive or classified information, when printed, shall be cleared from printers immediately. Where possible printers with a “locked job” facility shall be used.

It is good practice to lock all office areas when they are not in use. It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

Any visit, appointment or message books shall be stored in a locked area when not in use.

The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.

ii. Clear Screen

KEPHIS's computers / computer terminals shall not be left logged on when unattended and shall be password protected.

Computer screens shall be angled away from the view of unauthorized persons.

The Windows Security Lock shall be set to activate when there is no activity for a short pre-determined period of time.

The Windows Security Lock shall be password protected for reactivation.

Users shall log off or lock their machines (by pressing the Ctr— Alt+ Delete key) when they leave the equipment unattended.

18.0 Teleworking Policy

Definition: Teleworking — Working from a site other than the employee's usual and customary work site (primary workplace). The alternative workplace shall include the employee's home.

The following guidelines shall be adopted during teleworking

- i. Teleworking equipment provided by KEPHIS and not in the local domain shall only be modified or replaced if authorized by ICT department. (E.g. Tablets)
- ii. Teleworking equipment supplied by KEPHIS is only to be used by the institution staff, particularly since others are not bound by institution's agreements and policies.
- iii. Only when unavoidable staff may take, send or print hardcopies of confidential documents out of secure KEPHIS locations. Where absolutely necessary to handle confidential hardcopy documents they shall be kept in locked cabinets when not attended (clear desk policy), sent by special delivery post, delivered by hand where possible and disposed of by shredding.
- iv. Staff, provided with computing and communications equipment for teleworking shall not put the information at risk by using other less secure equipment.

19.0 Business Continuity Management Policy

Information security continuity shall be embedded in the organization's business continuity management system. KEPHIS shall determine its requirements for information security and continuity of information security management in adverse situations.

- a) Business heads shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during adverse situations.
- b) The established and implemented information security business continuity procedures and controls shall be verified at regular intervals in order to ensure that they are valid and effective during adverse situations

20.0 Policy on Printers, Telephone Lines, and Copiers

The Staff are expected to use the above responsibly. Irresponsible/ excessive use of the above for personal purposes is discouraged, and shall, depending on the line manager's determination and management's approval lead to disciplinary action.

21.0 Review of the ICT Policy

The ICT policy shall be reviewed annually or if significant changes occur to ensure its continuity, suitability, adequacy and effectiveness.