



**JOMO KENYATTA UNIVERSITY OF  
AGRICULTURE AND TECHNOLOGY**

# **Information Security Policy (JISP)**

**ISO 9001:2008 Certified**



**2010**





Jomo Kenyatta University of Agriculture  
and Technology

# Information Security Policy (JISP)

ISO 9001:2008 Certified

## **Vision**

*A University of global excellence in Training,  
Research and Innovation for development.*

## **Mission**

*To offer accessible quality training, research and innovation  
in order to produce leaders in the fields of Agriculture,  
Engineering, Technology, Enterprise Development, Built  
Environment, Health Sciences and other Applied Sciences  
to suit the needs of a dynamic world.*

© JKUAT

JOMO KENYATTA UNIVERSITY OF  
AGRICULTURE AND TECHNOLOGY

P.O. BOX 62000 – 00200

CITY SQUARE

NAIROBI, KENYA

TEL: +254-67-52711, 52181-4

FAX: +254-67-52164

E-MAIL: .....@jkuat.ac.ke

WEBSITE: <http://www.jkuat.ac.ke>

# Contents

Definition of Terms	iv
1. Preamble	1
2. Introduction	3
3. Principles of Information Security	4
4. Responsibility for Information Security	5
5. Classification of Information	8
6. Access to Information	10
7. Standard Practices related to JKUAT's Information System	13
8. Production Systems Development	24
9. Control of Information Security	26
10. Departure from JKUAT	27

## Definition of Terms

- Access -** Permission to use an information resource
- Authentication -** Verification of the identity of a person or process in a communication system to ensure that messages really come from their stated source
- Encryption-** The process of making a message indecipherable in order to protect it from unauthorized viewing or use
- Firewall-** A security program that protects a network from computers outside the network, preventing unauthorized users from accessing the network
- Information custodian -** A person who retains physical or logical possession of an information resource on behalf of an information owner and serves users authorized by the owner
- Information owner -** A person charged with responsibility for deciding who and how an information resource may be used.
- Information security -** The protection of information resources and systems from accidental or deliberate damage, or unauthorized use.
- Information sensitivity-** The degree to which information is exposed to risk and must be handled with care or secrecy; JKUAT employs three categories of information based on level of sensitivity:

1. **Public:** information approved for general release, such as a press release or annual report.
2. **Internal Use Only:** information intended for use within the JKUAT by authorized persons only; such information may not be distributed publicly.
3. **Restricted:** private, reserved, confidential or otherwise sensitive information, access to which is limited to those with a legitimate JKUAT need; e.g. customer transaction accounts, staff performance evaluation records, reports of the outcome of internal investigations, legal information protected by attorney privilege and information related to crisis negotiation and staff security in crisis situations, among others.

**Information user** -A person who has authorized access to an information resource

**Non-compliance risk acceptance-** A signed request by a user for exemption from adherence to the information security procedures contained in this directive, including acceptance of any subsequent risks involved in non-compliance.

**Non-disclosure agreement** -A signed undertaking by a third party not to disclose information obtained from JKUAT to other parties

**Production system** -A system used to process JKUAT's information

**Remote computing** -Using telecommunications equipment to maintain contact with an office while working outside the office (e.g. at home or in the field)

**Sage ACCPAC System- Enterprise Resource Planning System** that forms the backbone of JKUAT's information system

**Telecommute** -To use telecommunications equipment to maintain contact with an office while working at home

**User-ID** -A unique name assigned to an individual user, identifying that user to an information system as being authorized

**User manager** -A person who approves a request for access to an information resource on the basis of a user's effective JKUAT needs as described in his/her job profile, and who is responsible for the activities of those authorized to gain access under his/her written approval

**Assets**- This refers to both hardware and software. It includes documents, files and information stored within file shares, databases, applications systems and services used to create, access, store and transmit this information. Also includes any other representation of this information regardless of medium (such as paper, diskette, CD-ROM, flash memory and magnetic tape).

**SDM**- This is the formal documentation for the phases of the system development cycle. It defines the precise objectives for each phase and the results required from a phase before the next one can begin. It may include specialized forms for preparing the documentation describing each phase.

# 1. Preamble

Jomo Kenyatta University of Agriculture and Technology acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. This obligation is shared, to varying degrees, by every member of the university.

Maintaining the security of information within the Jomo Kenyatta University of Agriculture and Technology (JKUAT) goes beyond the technology and concerns the entire organization – as computer-based support for JKUAT’s activities replaces manual procedures. Information management systems play an increasingly vital role in JKUAT’s activities; as such, the information contained in these systems is an institutional resource that requires adequate protection to guarantee operational effectiveness, efficiency, continuity and quality. JISP document is the framework policy document for all activities related to access to, and use of, all JKUAT information systems – it defines the rules necessary for secure and reliable access to JKUAT’s information systems.

By information security we mean protection of the University’s data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security policy is:

- \* To establish a University-wide approach to information security.
- \* To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.

- \* To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- \* To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

## 2. Introduction

This Policy has been developed to protect all systems within the University to an adequate level from events which may jeopardize University activity. These events will include accidents as well as behavior deliberately designed to cause difficulties.

Maintaining the security of information within the Jomo Kenyatta University of Agriculture and Technology (JKUAT) goes beyond the technology and concerns the entire organization – as computer-based support for JKUAT’s activities replaces manual procedures. Information management systems play an increasingly vital role in JKUAT’s activities; as such, the information contained in these systems is an institutional resource that requires adequate protection to guarantee operational effectiveness, efficiency, continuity and quality. JISP document is the framework policy document for all activities related to access to, and use of, all JKUAT information systems – it defines the rules necessary for secure and reliable access to JKUAT’s information systems.

### 2.1 Policy Statement

Jomo Kenyatta University of Agriculture and Technology will seek to ensure that the confidentiality, integrity and availability of its information is maintained by implementing best practice to minimize risk.

### 2.2 Scope

The measures described in this document apply to all JKUAT staff members and to anyone granted access to any JKUAT electronic information system.

## 2.3 Objectives

The objectives of this information security are to:

1. Protect information resources from unauthorized access;
2. Ensure the continuity of systems processing services;
3. Guarantee the privacy and accuracy of information resources;
4. Allow proper restoration of the functionality of damaged resources;
5. Prevent and detect possible threats, violations and security incidents.

## 3. Principles of Information Security

JKUAT bases its information security policy on four major principles: integrity, confidentiality, availability and accountability.

### 1. Integrity

Information stored in computer systems must be reliable, comply with standing policies, regulations and rules, and may only be created or updated by authorized persons.

### 2. Confidentiality

The content of information on computer systems must not be divulged to unauthorized persons in any form.

### 3. Availability

Information on computer systems must be available at agreed times to authorized persons who shall use this information exclusively in the performance of their official duties and responsibilities.

## 4. Accountability

The use of information on computer systems must be fully recorded in order to trace all forms of JKUAT activity back to originators.

## 4. Responsibility for Information Security

Activities related to the maintenance of information are performed by five classes of individuals:

1. Information owners
2. Information custodian
3. Information users
4. User managers

### 1. Information owners

Information resources used for JKUAT activities must have 'owners', who are JKUAT staff performing the following activities:

1. Authorizing access to information resources
2. Identifying categories of sensitivity for information.
3. Deciding how information shall be used and who shall use information
4. Defining acceptable limits for the quality of information (such as accuracy, timeliness and time from capture to use)
5. Identifying data retention periods and special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures)
6. Reviewing reports that indicate how information is being used and by whom

## 7. Designating a system-of-record for information from which all management reports are derived

JISP Owners may not delegate their responsibilities to third parties (such as outsourcing firms) or to non-JKUAT staff members. Each information owner must identify a back-up person to act in cases of unavailability. In the absence of either the owner or the back-up person, the absent owner's manager shall be responsible for the owner's information resources.

## 2. Responsibility: Information custodians

Information custodians are members of JKUAT staff who retain physical or logical possession of information and/or information systems. Custodians operate systems on behalf of owners and serve users authorized by owners. Custodians define technical options such as categories of information sensitivity to be selected by owners. Custodians define information system architecture and provide technical consulting assistance to owners in order that information systems are built and run in such a way as to best meet JKUAT objectives.

On request, custodians provide reports to owners about information system operations and availability. ICT is considered the main custodian of JKUAT's information assets, since most information is processed on computing facilities managed and maintained by the department. If the designation of a custodian is not clear on the basis of existing information system operational arrangements, the Chief Information Officer (CIO)/Head of ICT shall designate a custodian in line with the needs.

## 4.3 Responsibility: Information users

An information user is any person who has been authorized by JKUAT to use its computer facilities. User access is based on a user's job profile and is granted by a user manager. Users shall be assigned

user-IDs in order to gain access to information systems. Users are required to familiarize themselves and act in accordance with all JKUAT's information security procedures. They are also required to participate in information security training and awareness sessions, and report any suspicious activity or security problem.

#### **4.4 Responsibility: User managers**

User managers are JKUAT staff that approves system access on the basis of a job profile. If a job profile does not exist, the user manager is responsible for creating the profile and, obtaining the approval of relevant owners. User managers are responsible for the activities of staff, consultants and temporary assistants authorized to gain access to JKUAT's information systems under their written approval.

When a user ceases working on a job for which access privileges have been granted, the user manager is responsible for promptly informing ICT that the privileges associated with that person's user-ID must be terminated. User-IDs are specific to individuals, and may not be reassigned to, or used by, others.

#### **4.5 Responsibility: ICT security staff**

The security staff of ICT are responsible for all issues related to JKUAT's information security and currently reside in ICT's Administrative Services (ICTAS). This group proposes information security recommendations to senior management, taking into account the needs of various owners, managers, custodians and users. Upon management approval, the group implements information security standards, procedures and policies. The group is responsible for coordinating all activities related to administration of access control, monitoring the security of JKUAT's information systems and providing information security training. The group carries out regular security control and provides management

with reports on the current state of information security within the JKUAT. The group is responsible for organizing a computer emergency response team (CERT) to respond promptly to security issues, such as virus-based infections and break-ins.

## 5. Classification of Information

To ensure appropriate and sound handling of information throughout JKUAT, different levels of information are classified according to sensitivity – that is, the degree to which they are exposed to risk and must be handled with care or secrecy. All information resources must be labeled clearly by category of sensitivity and handled according to the relevant procedures established in this directive. One important objective of a sensitivity classification system is to provide consistent handling of information resources, no matter what form they take, where they go and who possesses them. JKUAT uses three categories to classify the sensitivity of information on the basis of level of confidentiality:

- \* Public
- \* Internal Use Only
- \* Restricted

### 1. Public information

This is information that may be made available to or consulted by anyone who has a legitimate need for such information in JKUAT. Information may only be disclosed to the public if it carries a 'Public' label and the information owner has given written approval, or if it is the type of material that is part of a long-standing practice of public distribution. In the case of public fora such as Internet, the VC, must approve JKUAT materials for publication. Internal Use Only information is information that may only be made available to or consulted by JKUAT staff members or authorized

recipients (examples include the JKUAT Telephone Directory and most internal e-mail messages). Information in this category is exclusively intended for use within JKUAT.

## **2. Restricted information**

This is information that has been so classified by its owner with the intention of limiting its distribution to a designated recipient(s) with a JKUAT-based need(s). Information in this category is confidential, reserved or otherwise sensitive. Restricted information includes, but is not limited to, minutes of meetings, customer transaction accounts, personnel records, staff performance evaluation records, reports of the outcome of internal audits and investigations, legal information protected by attorney privilege and information related to crisis negotiation and staff security in crisis situations, among others. Unauthorized disclosure of Restricted information to persons without a legitimate JKUAT need for access is not permitted and could result in disciplinary action, applicable under existing staff regulations and rules, as well as relevant guidelines. Restricted information must not be stored on PCs but on servers that are adequately protected, monitored and controlled by ICT through secure centralized mechanisms and procedures.

### **5.3 Internal Use only**

Information not classified under one of the above three categories shall be automatically classified under the Internal Use Only category. It is not necessary to apply a sensitivity label for Internal Use Only information.

Owners of information are responsible for designating the appropriate label for each information resource; users of information are responsible for ensuring that the correct label is maintained for each information resource. Labels for Internal Use Only and Restricted information shall be used for email messages or printed

memos. They shall appear on storage media such as floppy diskettes or CD-ROMs.

In cases where an information resource has been compiled from more than one source, and these sources carry different levels of sensitivity, the composite information resource must carry a label corresponding to that of the source with the highest level of sensitivity; for example, if a document has been compiled from Public and Internal Use Only information, the document must be labeled Internal Use Only.

The level of sensitivity of an information resource may change over time. For example, a document originally intended for executive staff use only (Restricted) may be edited for eventual public dissemination, in which case it shall be re-labelled as Public information. Information owners are responsible for the decision to re-classify information resources.

Restricted information and all software to handle it must be erased from disks, tapes or other magnetic storage media by repeated overwrite operations that prevent the data from being retrieved at a later date.

## **6. Access to Information**

There are no restrictions on access to Public information for those with a legitimate need, nor on access to Internal Use Only information for users authorized to consult such information. Access to Restricted information shall only be granted if:

1. A legitimate JKUAT need has been demonstrated, and
2. Authorization has been obtained from the relevant information owner.

The relevant manager must initiate the access approval process for a new user.

All users shall automatically be granted basic information systems services, such as word processing facilities.

Access to all other system capabilities shall be determined on the basis of job profiles or by special request directed to the owner of the information involved. The access privileges granted shall remain in effect until the user's duties change or he/she no longer works for the JKUAT. If either of these two events takes place, the manager must immediately notify ICTA in writing.

In the case of a change in a user's duties, and following notification of this change by the manager concerned, ICTA shall activate new levels of access on the basis of the user's new job profile. All non-employees (such as contractors, consultants, volunteers and outsourcing firms) must go through an access request and authorization process, which is initiated by the relevant JKUAT manager. The privileges of these non-employees must be immediately revoked through ICTA on termination of the contractual period or when duties change.

A non-employee shall only be granted limited information system services (such as word processing facilities) and shall be strictly monitored; depending on legitimate needs, the manager involved may authorize access to other services. The fact that certain access privileges exist does not necessarily mean that they shall automatically be granted in all cases. Any questions about access privileges shall be directed to ICTA. ICTA or a delegated ICT staff shall assign a unique user-ID to each user, and this user-ID shall follow an individual as he/she moves through JKUAT. User-IDs

shall be permanently terminated when users leave JKUAT. Re-use of terminated user-IDs is not allowed. User-IDs are linked to specific individuals and are not associated with computer terminals, units or job titles. Anonymous user-IDs are not allowed.

All information system user-IDs must have a linked password or a stronger mechanism (such as a dynamic password token) to ensure that only the authorized user is able to use the user-ID. Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism).

Users must immediately notify ICTA and change their password if they suspect that it has been discovered or used by another. Likewise, users must notify ICTA if other access control mechanisms have been broken or if they suspect that these mechanisms have been exposed to a breach of security.

To prevent unauthorized persons from using the access privileges associated with a user-ID, users must ensure that they log off from multi-user computers when they leave their desks for extended periods.

Dormant user-IDs, which have not seen any activity for a period of three (3) months, shall have their accounts and all related files archived.

Users who return from leave of absence must have their manager request reestablishment of their access privileges if these have been revoked in the meantime.

## 7. Standard Practices related to JKUAT's Information System

This section describes the standard practices regarding access to, use of and rights related to use of the JKUAT information system and covers the following:

- Passwords and access:
- Password management,
- Third party access,
- Encryption
- Use of information services
- Network connections
- Internet
- E-mail
- Remote computing and home-based work
- Viruses, malicious software and change control
- Printing, photocopying and fax transmission
- Privacy and rights
- Protection of third party information
- Intellectual property rights
- Passwords and access: Password management
- Passwords authenticate the identity of users.

Users must not share a password with anyone, including their manager or colleagues. If a user needs to share information with others, he/she must employ authorized mechanisms, such as protected directories or diskettes. Users should choose easy-to-remember and difficult-to-guess passwords. This usually means that passwords should not be work-related or reflect aspects of the

user's personal life (for example, a license plate number or spouse's name).

All passwords should contain at least six characters, and where systems support it, this minimum length should be enforced automatically. Users should also choose passwords that include both alphabetic and numeric characters. Where systems support it, passwords must be changed at least every 120 days. Likewise, where systems support it, administrators must force the change of 'initial access' passwords and oblige users to choose their own passwords. 'Initial access' passwords are the passwords that appear the first time an application is opened. Passwords must not be reused. If a user suspects that another person knows his/her password, he/she must change the password immediately and inform ICTA at JKUAT or the delegated ICT officer in JKUAT offices for further control. The person responsible for password authorization must authenticate the identity of a user before re-setting his/her user password. Users must not store their passwords in any computer files (such as log-in scripts or computer programs) unless the passwords have been encrypted with authorized encryption software (see section on Encryption below).

Likewise, passwords must not be written down unless a transformation process has concealed them, or they have been physically secured (such as placed in a locked filing cabinet). The custodian of the system must change any password set by vendor default before it can be used for JKUAT's activities.

## **1. Passwords and access**

### **7.1.1 Passwords and access: Third party access**

Before third party users are permitted to access JKUAT's private systems via real-time computer connections (such as dial-up lines, Internet and value added networks), written approval must be

obtained from ICTA or a delegated ICT officer at regional bureau/ country office level. These third parties include information providers, business partners, and contractors and consultants working on special projects.

Third party information system firms must only be given inbound connection privileges (such as dial-up and Internet) after ICTA at JKUAT or a delegated ICT officer at JKUAT has verified a legitimate business need. These privileges must be available only for the period of time required to accomplish previously defined and approved tasks.

On departure of members of their staff who have been granted access privileges, third parties shall notify JKUAT.

Unless the relevant information owner has given prior approval, users must not place anything other than JKUAT Public information in a directory, on a server, or at any other location where unknown parties could gain ready access; an example is the posting of sensitive files on an Internet-connected server that could be accessed by third parties.

A condition for granting third party access to JKUAT's computer network is that these parties must secure their own connected systems in a manner consistent with the procedures contained in this directive.

JKUAT reserves the right to audit the security measures in effect on third party connected systems. JKUAT also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements. These rights shall be stipulated in each single contract between JKUAT and a third party system.

## **7.1.2 Passwords and access: Encryption**

Encryption refers to the process of making a message indecipherable in order to protect it from unauthorized viewing or use. Whenever Restricted information is sent over a public computer network such as Internet, a secure network should be used to protect such information. Whenever restricted information is stored in a computer, this must be done using authorized encryption methods. Information owners must define these circumstances in greater detail. Many encryption routines require that the user provide a key as input. Users and custodians must protect these security parameters from unauthorized disclosure, just as they must protect passwords from unauthorized disclosure.

Rules for choosing keys shall follow the rules for choosing passwords. Since JKUAT's two major computer networks - the Local Area Network (LAN) and the Wide Area Network (WAN) – contain no pre-installed automatic encrypting mechanisms, users must take specific action themselves to have encryption facilities enabled if information must be protected. For example, confidential e-mail messages may be encrypted and digitally signed, and mechanisms may be put in place to prevent wiretapping of telephone conversations.

## **7.2 Use of information Services**

### **7.2.1 Use of information Services: Network connections**

Real-time connection between two or more in-house JKUAT computer systems must not be established unless it has first been determined that such a connection shall not jeopardize information security. Connection of ICT-managed desktops to the internal network does not require permission. Staff must not connect private computers to JKUAT computers or networks without prior authorization from ICTA.

Likewise, personally owned systems may not be used to process any JKUAT information unless these systems have first been approved for such use by ICTA at JKUAT.

Staff and consultants working for JKUAT must not make arrangements for, or actually complete, the installation of voice or data lines with any carrier, unless they have first obtained approval from ICTA,

JKUAT computers or networks may only be connected to third party computers or networks after verification that the combined systems shall comply with JKUAT's security requirements. With the exception of portable and telecommuting computers, the use of modems directly attached to, or integrated into, personal computers to establish communications sessions with JKUAT computers or networks shall be avoided.

All dial-up connections with JKUAT computers and networks must be routed through a modem pool protected by approved user authentication security mechanisms.

### **7.2.2 Use of information services: Internet**

While the public Internet offers great potential benefits, it also exposes JKUAT to significant risks due to the inherent lack of controls and personal misuse. The risks include exposure to destructive programs and unsolicited messages, among others. Authorized users have the responsibility to use Internet in a professional, lawful and ethical manner; they must ensure that their Internet-based activities are compatible with the ethical standards of the International Civil Service environment. Authorized users must also ensure that the duration of their use of Internet is limited to reasonable periods of time compatible with their professional duties and responsibilities. All connections between JKUAT internal networks and Internet must include an approved control system.

### 7.2.3 Use of information services: E-mail

E-mail accounts, like user-IDs, are issued for specific individuals and must not be shared. In exceptional cases, where the exigencies of service require a shared account, this must be documented in writing and copied to ICTA at JKUAT or the delegated ICT officer in its campuses or centres. If a user is absent or unable to check his/her mail for an extended period, mail shall be forwarded to another JKUAT staff member. At the same time, notices shall be created that shall automatically inform correspondents that the recipient shall not be responding for a certain period of time. Upon departure from JKUAT, a user's e-mail account shall be terminated.

To restrict the dissemination of sensitive information, no forwarding of e-mail to addresses outside JKUAT is permitted without a copy being saved in JKUAT's system. If an e-mail message contains sensitive information, users must not forward it to another recipient unless:

1. The recipient has been authorized to view the information; or
2. The originator has approved the forwarding.

Broadcast e-mail message facilities shall not be employed unless prior approval has been obtained from a JKUAT manager, but the use of selected distribution lists is both advisable and permitted. E-mail systems contain no pre-installed automatic encrypting mechanisms, since such mechanisms shall not be applied in all cases, especially outside JKUAT's LAN networks; therefore, users must be careful about including sensitive information in e-mail messages that are not protected by encryption.

E-mail messages are automatically recorded in logs and back-up systems. This means that even though an e-mail message has been deleted from a user's in-box, it may still be retrievable. Nevertheless,

because e-mail messages are periodically removed from the system and archived, individual users are responsible for saving important messages they think they may need in the future.

E-mail systems shall not be used as databases; users shall switch important messages from e-mail systems into other storage locations such as word processing documents.

#### **7.2.4 Use of information services: Remote computing and home-based work**

The security of JKUAT information and physical property at remote locations is as important as in JKUAT main campus office. If the remote user works with sensitive information, he/she must follow the same information handling procedures applied in JKUAT offices. Remote access to the JKUAT's information systems shall be granted only to those users with a demonstrable JKUAT need for such access.

Authorization for remote access to JKUAT computers is granted by and reviewed every six (6) months by ICTA at JKUAT or the delegated ICT officer at its campuses or centres. To ensure that the requirements for remote access are observed consistently, JKUAT reserves the right to conduct surprise checks of users with remote access privileges. Remote access to JKUAT computers and networks requires that all users be

Definitively authenticated with passwords or other approved identification systems.

All remote users must connect to JKUAT computers and internal networks via authorized communications systems such as firewalls. Inbound connection to JKUAT computers or networks through an office desktop

Modem shall be avoided unless specific approval has been obtained from ICTA or a delegated ICT officer. Leaving computer-linked modems in auto-answer mode shall be avoided unless an approved remote user identification system has been installed. Users must make sure that their files shall be remotely backed up over the network, or that they shall have appropriate remote systems to perform their own back-ups.

All portable and remote computers under the control of JKUAT staff, and which are used to process JKUAT's information, must be protected by an approved access control package. Access control packages prevent unauthorized use of computers and unauthorized access to JKUAT information. They also prevent virus infections and other types of damage caused by malicious software. In general, Restricted information shall remain physically within JKUAT's offices.

If it is necessary to remove computer-readable sensitive information from an office, such information must be protected with approved protection facilities. However, such a practice shall only be followed on a temporary basis. If sensitive information is transmitted over public computer networks such as Internet, this transmission must employ approved encryption facilities.

Information systems equipment used to handle JKUAT information shall be stored in a locked area. Because theft of such equipment is common, users must not store passwords, user-IDs or any other access information in portable or remote systems.

### **7.2.5 Use of information services: Viruses, malicious software and change control**

Approved virus-checking systems must be in place on all personal computers with operating systems susceptible to viruses and on all e-mail servers. All files from external sources must be checked

before execution or use; if encryption or data compression has been used, these processes must be reversed before starting the virus-checking process. Users shall not turn off or disable virus-checking systems.

If a user receives a virus alert, he/she must immediately disconnect from all networks, cease use of the affected computer, and call the Computer Help Desk for technical assistance. To prevent possible damage to JKUAT's information and information systems, users are not permitted to remove viruses on their own.

If a user believes he/she has been the victim of other malicious software, the Computer Help Desk must be contacted immediately in order to minimize the damage. User possession or development of viruses or other malicious software shall be avoided.

Users are not permitted to install new or upgraded operating systems or applications software on personal computers or other machines used to process JKUAT information. Systems used to process JKUAT information may or may not be owned by JKUAT, but have been specifically recognized as systems used for regular JKUAT activities.

These systems may offer automatic software distribution, automatic software license management, automated remote back-up and related functions on a centralized and coordinated basis. While software/system change control is maintained through the access control packages mentioned above, users may change preferences within software packages, such as the fonts in a word processing package.

### **7.2.6 Use of information services: Printing, photocopying and faxing**

When printing sensitive information, a user must:

1. Be present at the moment of printing to prevent the information from being revealed to unauthorized parties; or
2. Direct the output to a printer inside an area to which only authorized staff have access.
3. A dedicated printer shall be used for units/offices managing Restricted information.
4. Since material contained in magazines, journals, newsletters and other publications is normally protected by copyright, permission shall be obtained from the copyright owner(s) before making multiple photocopies, if necessary.
5. Sensitive material must not be faxed unless:
  1. An authorized staff member is on-hand at the time of transmission to properly handle the material at the receiving site;
  2. The fax is sent to a locked room to which only authorized staff have access; or
  3. A password-protected fax mailbox is used to restrict release to an authorized recipient.
  4. All faxes must employ a standard cover page that contains approved wording.
  5. Third party signatures on contracts, purchase orders and similar legal documents sent by fax must always be followed up with an exchange of paper originals.

If a printer, copier or fax machine jams or malfunctions while printing, photocopying or transmitting Restricted information, users must not leave the machine unattended until all copies of the

information have been removed or are no longer legible. All paper copies of sensitive information must be disposed of by shredding or other approved methods.

## **7.3 Privacy and rights**

### **7.3.1 Privacy and rights: Protection of third party information**

A wide variety of third parties (including many development partners) have entrusted their information to JKUAT, and all users at JKUAT must do their best to safeguard the privacy and security of this information.

Whenever activities with third parties necessitate the release of sensitive JKUAT information, the third party must sign a 'non-disclosure agreement', an undertaking not to disclose information obtained from JKUAT to other parties. Information released to these third parties must be limited to the topics directly related to the project or operational relationship concerned.

All outsourcing contracts shall include clauses covering the registration of users and the right of JKUAT to audit compliance with JKUAT's security requirements.

### **7.3.2 Privacy and rights: Intellectual property rights**

With the exception of material clearly owned by third parties, subject to JKUAT Intellectual Property Rights, JKUAT is the legal owner of all JKUAT information stored on or passing through its systems. All JKUAT-related information developed while at JKUAT as a user is JKUAT property. Users must not make copies of or use software unless they know that the copies comply with the license signed between a vendor and JKUAT.

If a system that is used to process JKUAT's information has been installed, users must ascertain that all software on that system has been licensed and authorized. Questions about licensing shall be directed to ICT department, which maintains documentation on software licenses throughout JKUAT.

Making regular back-ups of software for contingency planning purposes is permitted. Such back-ups shall be stored in a safe location, where possible outside the office premises. Any unauthorized software installed on a 'system that is used to process the JKUAT's information' shall be removed and the person(s) concerned could be subject to disciplinary action, applicable under existing staff regulations and rules, as well as relevant guidelines.

This section is subject to JKUAT Intellectual Property Rights.

## 8. Production Systems Development

'Production system' refers to a system that is used to process JKUAT's information. Although a production system may be physically situated anywhere, production system designation is carried out by ICT at JKUAT or a delegated ICT officer. Information systems that have been designated 'production systems' carry special security requirements. All software created in-house that runs on production systems must be

developed according to the System Development Method (SDM). Among others, this methodology ensures that the software is adequately documented and tested before use with JKUAT information. SDM also ensures that production systems include adequate control measures. Production systems must also have designated owners and custodians for the essential information they process. Periodic risk assessments of production systems shall be carried out to determine whether the controls in use are

adequate. All production systems must have an access control system to monitor and restrict access privileges.

ICT department at JKUAT or a delegated ICT officer at its campuses and centres assigns an access control administrator for each production system. There shall be a separation between production, development and test environments.

This ensures that security is maintained in a much more rigorous way for a production system, while the other two environments shall maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted access to production systems.

All production software testing must be carried out with sanitized information (where Restricted information is replaced with dummy data).

All security fixes provided by software vendors must also go through the SDM testing process, and must be promptly installed. A formal and documented change control process must be used to restrict and approve changes to production systems.

Application programmers must not be given access to production information. All application program-based access paths, other than the formal user access paths, must be deleted or disabled before software is moved into production.

Detailed documentation of application must be lodged with ICTA for security assessment. Production systems shall be located in a lockable room with access limited to authorized personnel.

Maintenance procedures must be regulated by written instructions.

Users are not permitted to write production computer programs, unless specifically authorized. The construction of spreadsheet formulae, databases or automatic execution scripts that are run when a system is booted is not considered programming for the purposes of this directive.

Both users and programmers must be careful never to embed user-IDs or readable passwords in any file.

## **9. Control of Information Security**

### **9.1 Control: Reporting problems**

All users must promptly report any theft or loss of, or severe damage to, hardware or software to the Computer Help Desk.

Users shall also report all suspected compromises to JKUAT's information systems. For instance, if a hacker is believed to have broken into the JKUAT systems, this must be reported.

If a situation of serious information security vulnerability is known to exist, this must also be reported.

All cases of suspected disclosure of Restricted information must be reported to ICTA or a delegated ICT officer at Campuses/centers.

Staff with questions about information security (for example, a user wondering whether a certain action would jeopardize security) shall call ICTA.

Reports must not be sent by e-mail unless the message has been encrypted with authorized software.

## 9.2 Control: Non-compliance risk acceptance

Non-compliance with these and other information security requirements may result in action, up to and including termination of service.

In rare cases, a JKUAT case for non-compliance may be established; in such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process calls for the signing of a request for non-compliance by a unit/section manager and approved by ICTA.

## 10. Departure from JKUAT

Managers are responsible for notifying ICTA of all staff terminations as soon as possible. When an individual with access privileges leaves JKUAT, all system access rights shall be terminated upon departure. The manager of the departing staff member must notify ICTA of the status of documents stored on shared servers, the departing staff member's PC and the e-mail repository. Unless otherwise notified, ICTA shall archive and delete all documents from these locations.

A manager may decide to maintain a departing staff member's e-mail account active for a period of up to 4 (four) months for the purposes of business continuity. In this case, the manager must designate who shall monitor the departing staff member's e-mail account for business communication. It is up to the departing staff member's manager to notify all business contacts of the staff member's departure. All information products prepared by users for JKUAT are the property of the JKUAT, and must remain with JKUAT when a user departs; for example, a computer program written by a member of the Information Systems Development Branch (ICTD) while employed by JKUAT is JKUAT property and must remain with JKUAT.

E-mail documents of value for JKUAT shall be saved in a secure location where they shall be accessed when needed.



## **Jomo Kenyatta University of Agriculture and Technology**

P.O Box 62000-00200, Nairobi, Kenya

Tel: 254- (0)67-52711

Fax: 254-(0)67-52164

Website: [www.jkuat.ac.ke](http://www.jkuat.ac.ke)