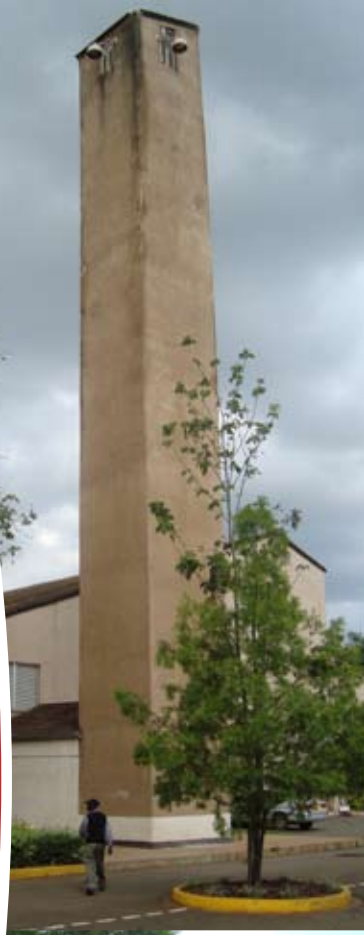
JOMO KENYATTA UNIVERSITY OF
AGRICULTURE AND TECHNOLOGY

Security Policy or JKUAT Electronic Payments

ISO 9001:2008 Certified



2010

Jomo Kenyatta University of
Agriculture and Technology

Security Policy or JKUAT Electronic Payments

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.

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

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

JEPS JKUAT Electronic payment system

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:

Restricted: Private, reserved, confidential or otherwise sensitive information, access to which is

limited to those with a legitimate corporate need.

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

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

Remote computing Using telecommunications equipment to maintain contact with an office while working outside the office (such as at home or in the field)

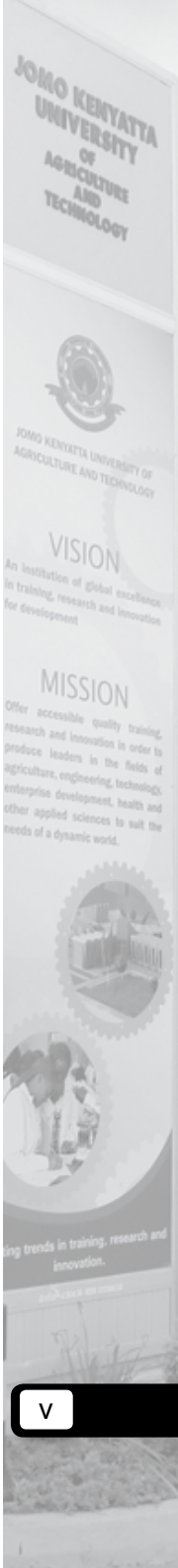
User-ID A unique name assigned to an individual user, identifying that user to information system as being authorized

1. Preamble

The manual processing of payments and interaction with third party financial institutions has been replaced in JKUAT by computer-based electronic payment systems (JEPS). These play a vital role in ensuring the operational quality, integrity, efficiency and continuity of JKUAT's activities and operations, and as such require effective security measures.

This 'Security Policy for JKUAT's Electronic Payment Systems' document defines the rules necessary for secure access to and correct use of JKUAT's payment systems, and is in line with the principles and rules established in the following framework policy documents:

1. JKUAT's Corporate Information Security Policy – to be developed
2. ISO 9001:2008 Finance Procedure Manual
3. Central Bank Regulations and procedures
4. Any Regulations from Government and the Laws of Kenya



2. Objectives

The overall objective of this policy document is to provide rules and specific good practice guidance for the security and control of JKUAT's electronic payment systems.

The specific objectives are to:

1. Identify operational rules for the correct use of JEPS
2. Protect information resources from unauthorized access
3. Assure the privacy and accuracy of banking operations
4. Prevent and detect possible threats, violations and security incidents
5. Prevent financial risks such as unauthorized payment or theft
6. Ensure the continuity of JEPS processing services

3. Principles

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

Integrity

Payments operations comply with standing policies, regulations and rules, and may only be created or updated by authorized persons.

Confidentiality

The content of payments shall not be divulged to unauthorized persons in any form.

Availability

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

Accountability

The use of information on JEPS shall be fully recorded in order to trace activity back to originators. The requirements set out in this document are considered generic to good practice and control, irrespective of the system to which they are applied.

4. Responsibilities

To ensure a high level of integrity and accountability for JEPS operations, it is vital that responsibilities and roles are properly defined.

Four key roles have been identified to provide a hierarchical level of control in relation to electronic payment systems:

1. System owners
2. System users
3. User managers
4. System administrators

All members of staff using (including systems administrators) JEPS shall take an oath of office.

4.1 System owner

The system owner for JKUAT's electronic payment system is the Vice Chancellor.

The system owner is responsible for defining the job profiles of users, which includes but is not limited to:

1. Functions they shall perform (payment processor or authorizer, bank accounts, currency, etc.)
2. Limits to release payments
3. Control settings

Users are granted JEPS access only under the written authorization of the system owner. When a user ceases working on an JEPS job for which access privileges have been granted, the system owner is responsible for promptly informing the system administrators that JEPS privileges shall be terminated. The owner reports cases of operational misuse or errors and security problems, and in collaboration with the authorizer and system administrators takes action for further checks and rectification.

4.2 System users

JEPS information users are those JKUAT staff members authorized to process electronic payment operations. The users are finance staff in JKUAT and its compuses/Cetres.

There are two levels of user:

4.2.1 Inputter: A user who carries out the routine input functions of the electronic payment system and performs clerical duties such as data entry, reporting, control of operational transactions flows, documentation and back-up of operational data.

2. Authorizer: A user, who authorizes payments, liaises with financial counterparts, controls the correctness

of payments execution and the status of accounts, and reviews operational logs.

More than one level of authorization may be used in JEPS. JEPS users' job descriptions shall include JEPS functions and responsibilities, and shall be signed by staff members as acceptance of associated responsibilities. A copy of a user's job description shall be held permanently on his/her personnel file. To ensure that all JEPS users are aware of operational procedures, and working policies and practices, they shall receive appropriate training and periodic reminders.

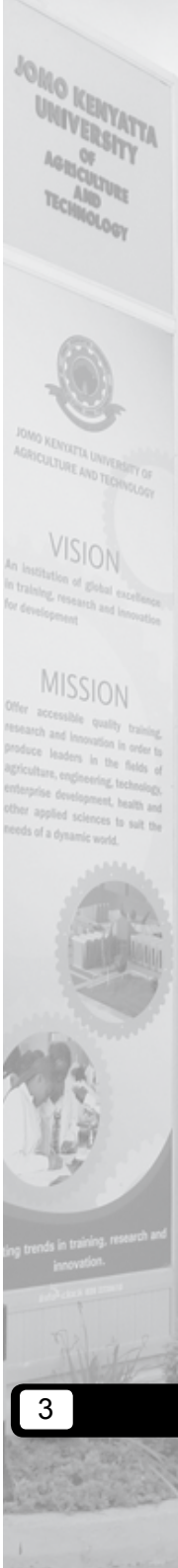
3. User managers

User managers are JKUAT Deans/Directors/Managers/CODs/HODs that request access to the JEPS system for their staff members. User managers are responsible for the activities of staff authorized to access JEPS 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 the owners and the system administrators that the privileges associated with that person's user-ID be terminated. User managers authorize any extension to access the JEPS system beyond standard local working hours.

4. System administrators

System administrators are responsible for the control and the correct functioning of all aspects related to technology and security requested by the electronic payment services. The administrators are responsible for all activities related to administration of security, such as:

1. Security configuration of JEPS systems



2. Profiles
3. Security Policy for JKUAT's Electronic Payment Systems
4. Users and their privileges
5. Libraries
6. Physical and logical security
7. System administrators carry out regular security control activities and provide the system owner with reports on the current state of JEPS security and use, including:
    1. Review of security logs
    2. Control of physical access
8. System administrators take care of installing, maintaining and controlling JEPS systems and the JEPS environment (such as networks, Internet connections, modems and physical access).
9. Liaising with bank technical support
10. Installing and maintaining JEPS software and devices
11. Administering the configuration of JEPS computers
12. Acting as a valuable resource to employees who may ask for technical assistance
13. Controlling any system changes
14. Integrating JEPS with back office systems and controlling correct functioning.

Following approval from the system owner, and in collaboration with users and managers, system administrators are responsible for issuing JEPS technical policies, procedures and manuals. The system administrators' responsibilities reside with the head of the JKUAT ICT department.

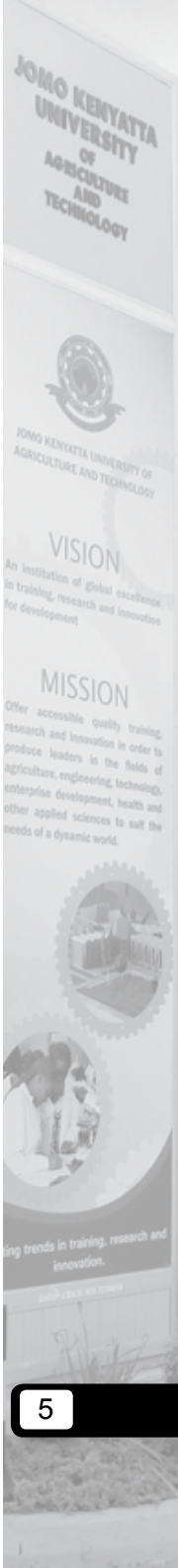
5. Segregation of Duties

The segregation of duties within an application system reduces the risk of unauthorized actions, whether accidental or deliberate. Segregation of duties is maintained by logically separating the functions that any one person shall carry out within JEPS application, thus avoiding control of the entire process by any single person.

To maintain segregation, dual authorization control is applied. Under dual authorization control, the performance of sensitive actions requires two separate individuals: one to initiate an action and the other to authorize (approve) the action.

1. Rules of segregation

1. System ownership, information use and system administration are separate functions.
2. The principle of dual authorization control is applied to the execution of all payments or transfers; thus, inputting and authorizing are separate functions.
3. Two levels of authorization are necessary to release a payment; in both cases, this involves digital release or confirmation fax to banks.
4. Restrictions may be placed on the bank accounts that inputters and authorizers shall operate.
5. Dual authorization control security is applied for the actions of system administrators when modifying JEPS system or user configuration.
6. The amount an authorizer shall release may be limited; the system owner establishes the payment authorization ceiling assigned to each authorizer.



Dual authorization control is not required for reports of balances and transactions, manual inputting of transactions or uploading of batch payment files, or wire/fax sending of payments, even if information shall be protected by security and treated with confidentiality.

6. Classification of Information

To ensure appropriate and sound handling of information processed through electronic payment systems is classified as "restricted". As such, JEPS information is considered confidential and its distribution is limited to designated recipients only.

All users accessing JEPS information shall do their best to safeguard the privacy and security of this information. Unauthorized disclosure of information related to payments is not permitted and

shall result in disciplinary action, applicable under existing staff regulations and rules, as well as relevant guidelines. The security procedures and rules set out here aim to ensure consistent handling of JEPS information.

7. Access to Information/User authorization

Since electronic payment systems are multi-user information systems, it is necessary to maintain a formal user registration and de-registration procedure for granting access and managing privileges. Definition of access profiles and access to the system is responsibility of the system owner, who is required to authorize each user and his/her profile for operating within the system. All requests for access to the system shall be directed to the designated system administrator on an approved form.

The system owner shall be responsible for maintaining a table of access profiles, which define the user profile for each electronic payment system, and the actions that users with this profile are allowed to execute. Access privileges granted shall remain in effect until the user's duties change or he/she no longer works for JKUAT. If either of these two events takes place, the user manager shall immediately notify the system owner and system administrators in writing.

Non-employees (such as contractors, consultants, volunteers and outsourcing firms) shall not have access to JEPS business functions. To ensure that security is maintained in a rigorous way, JEPS systems with operational data shall not be used for testing purposes and programmers shall not be given access.

7.1 User-ID

JEPS user shall be identified by a unique user-ID. User-IDs are specific to individuals, and may not be reassigned to, or used by, others. Use-IDs shall be assigned by system administrators upon request of the system owner. Since, user-IDs are linked to specific individuals, they shall not be associated with computer terminals, units or job titles. Anonymous user-IDs or re-use of terminated user-IDs are not allowed. When possible, the user-ID shall conform to the following format:

User ID Format: 11112333

Where 1 = First 4 characters of Last Name

2 = First character of First Name

3 = Office Identifier

User-IDs shall be linked to a password and, when possible, also to a stronger mechanism (such as a dynamic password token) to ensure that only an authorized user is able to use a user-ID.

When technically possible, additional authentication methods shall be used to protect JEPS applications; these may include personal identification devices such as magnetic cards, key locks and dynamic password tokens. Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism).

7.2 Password management

Passwords authenticate the identity of users. The minimum password length for JEPS is 8 digits. Passwords shall be changed at least every 30 days. Where forced change is not an automatic system function, users shall change their password manually every 30 days. To enforce this control, system administrators shall require users to certify by signature that this change has been effected. Users shall not recycle previously used passwords. Where this shall be automated, the system shall retain a history of five generations. Four incorrect password attempts shall be allowed at log-in before the system revokes the user-ID. Users shall choose easy-to-remember and difficult-to-guess passwords. This usually means that passwords shall not be work-related or reflect aspects of the user's personal life (for example, a licence plate number or spouse's name). Users shall also choose complex passwords that include both alphabetic and numeric characters, and a mixture of upper and lower case characters. New users logging on for the first time shall immediately change their initial password. Users shall 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. Likewise, passwords shall 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).

System administrators shall change any passwords set by vendors or banks. System administrators shall authenticate the identity of a user before re-setting his/her user password.

Users shall not share a password with anyone, including their manager or colleagues. Users shall immediately change their password and notify the system administrator concerned whenever there is an indication that their system or password has been compromised.

Where JEPS applications have automatic enforcement for the passwords settings above (i.e. initial passwords, complexity, length, history, etc.), these shall be activated.

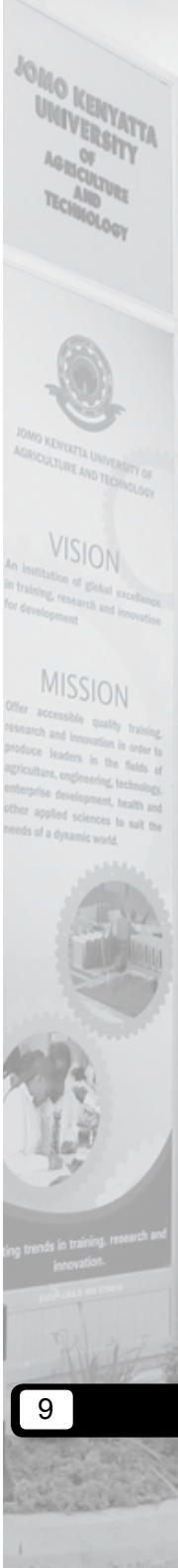
7.3 Authorizers and system administrator IDs

Where JEPS system does not allow two levels of system administrators or user authorizers, compensatory control for the segregation of duties is governed by the following rule:

The unique account's password shall be maintained in two parts; each half for each of the two administrators/authorizers'. It is the responsibility of each password holder to ensure that the secrecy of his/her half of the password half is maintained during the initial setting and subsequent entry process. Where access to a payment system is required, both persons shall be present to start a session.

7.4 Physical and Environmental Security

It is essential that resources used for the processing of electronic payment transactions are protected by both physical and logical security measures.



7.5 Perimeter security for JEPS computers

The overall security of the premises from which JEPS system operates is a corporate responsibility. However, it is the responsibility of system administrators to ensure that the following security perimeter measures are in place.

1. JEPS resources shall be located in an area that is not accessible to the public; the room housing these resources shall be protected by appropriate entry controls to ensure that only authorized JKUAT staff are allowed access.
2. The door to the secure area shall be locked when unoccupied and shall have a secondary locking device, such as a swipe card reader or push button/electronic code lock.
3. All windows shall be closed and locked when the room is unoccupied.
4. Where the secure area is located on the ground floor or adjacent to any roofing structures which may allow access, additional protection (such as bars or lockable shutters) shall be considered.
5. The secure area shall have appropriate fire detection and prevention mechanisms in place.
6. Where the building does not support a security alarm system, the door to the room shall have additional protection such as a lockable security device.
7. All JEPS resources shall be located away from potential environmental hazards such as overhead water pipes and sources of heat.
8. Local physical environmental conditions shall be monitored to ensure that they not have an adverse effect on JEPS operations. These conditions may include but are not limited to:

1. Dust
2. Ambient temperature fluctuations
3. Humidity
4. Electrical supply interference
5. Electromagnetic radiation

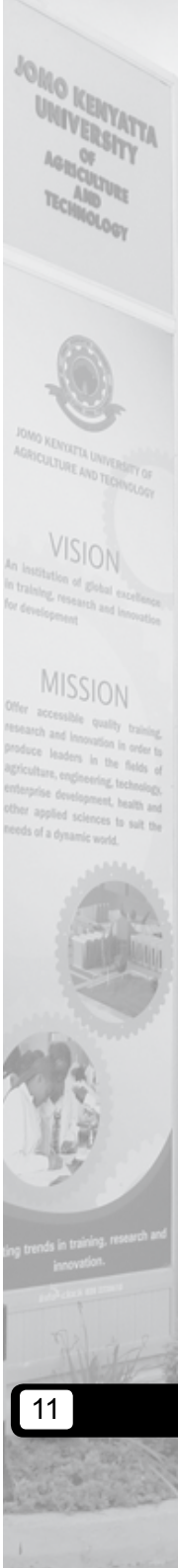
Since "restricted" information shall remain physically within JKUAT's offices, the use of JEPS systems from remote locations is not permitted.

7.6 Clear Desk / Clear Screen

In order to reduce the exposure to risk arising from unauthorized access, or loss of or damage to JEPS information, a user shall ensure that:

* When leaving JEPS workspace, all sensitive and confidential paperwork or other media (such as floppy discs, CD-ROMs) containing JEPS information are removed from the desk to either a lockable drawer or cabinet.
* When leaving JEPS workstation either during or at the end of a processing session, his/her session is correctly logged out, and the screen cleared to the desktop or a screensaver activated.

If it is necessary to remove sensitive information from an office, such information shall be protected with approved protection facilities; however, such a practice shall only be followed on a temporary basis.



7.7 Printing, photocopying and faxing

A dedicated printer shall be attached to a computer with JEPS application installed. The printers and fax machines used by JEPS staff shall be dedicated and located in the same security perimeter as the JEPS processing facilities. Any JEPS information sent to print shall be removed from the printer/fax immediately, and destroyed if not required for file evidence. The printer/fax tray shall be clear at the end of the day and the printer turned off. All paper copies of JEPS information shall be disposed of by shredding or other approved methods. Labels for "restricted" information shall be used for printed/ faxed memos. They shall appear on storage media such as floppy diskettes or CD-ROMs.

7.8 JEPS computers

JEPS information and software shall not be stored or run on end-user desktops but on dedicated computers that are adequately protected, monitored and controlled. In order to provide the maximum protection, JEPS computers shall have boot security enabled. JEPS applications shall have the ability to automatically close the session/connection after a defined period. If JEPS application does not have this as a built-in feature, a screen saver may be used as a compensatory measure.

In disposing of JEPS media, JEPS information and software shall 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.

7.9 Power supply

Due to the potential damage that power surges and outs shall cause to the integrity of data and continuity of service, it is important that:

* The offices hosting JEPS machines have an adequate back-up power facility, such as a generator.
* JEPS machines have a suitable uninterruptible power supply (UPS) fitted.

7.10 Time restrictions

To reduce the risk of exposure to unauthorized use, access to payment systems is allowed only during local office working hours, when offices are occupied and physical protection (such as guards) is active. Time restriction shall be enforced by implementing several methods of control, such as:

- locked doors
- secondary locking devices with time/date restrictions
- time restriction controls built in to an JEPS application

Time restriction controls shall not be seen as a substitute for the requirement to log out from an electronic payment system when not in use. They shall be seen as complementary/ compensatory controls in cases where JEPS application does not meet security requirements. Any extension to standard working hours shall be authorized by local managers, and access properly logged.

8. Logical Security/Network isolation of JEPS systems

JEPS systems shall not only be protected by physical measures but also by logical security measures such as network isolation and perimeter barriers such as firewalls, encryption mechanisms and dedicated modems. JEPS systems shall be installed on dedicated machines where no other applications are executed. Personally-owned desktops/laptops may not

be used to process JEPS information. JEPS machines shall be isolated: they shall not be accessible from public networks or from office LAN desktops/servers. Real-time connections are allowed only between JEPS machines and servers hosting financial back-office operations. These connections may be controlled via authorized communications systems such as firewalls. These connections shall always originate from JEPS machines; as a result, network devices shall never accept connections originating from external sources and destined for JEPS computers.

JEPS computers are connected to remote bank servers via private or public networks. In both cases, they may only be connected to remote bank computers or networks after verification that the communication set up complies with JKUAT's security requirements. Dial-up connections to private/public networks shall be allowed only through dedicated phone lines and modems pools. Lines shall be configured not to accept dial-in connections. This shall be achieved through ad-hoc filters set at the switchboard or modem level. JEPS modems shall be dedicated and not configured in auto-answer mode. All dial-up connections with remote computers and networks shall be routed through a modem pool authenticating the JEPS connections.

9. Authentication and encryption

Encryption refers to the process of making a message indecipherable in order to protect it from unauthorized viewing or use. Whenever payment instructions are sent over a public computer network such as Internet, or stored in a computer, this shall be done using authorized encryption methods. Many encryption routines require that the user provide a key as input. Users and administrators shall protect these security parameters from unauthorized disclosure, just

as they shall protect passwords. Rules for choosing keys shall follow the rules for choosing passwords (described in the section on Password management above).

10. Use of information services: Internet

If JEPS information is transmitted over public computer networks such as Internet, this transmission shall employ state-of art encryption and communication mechanisms. If technically possible, encryption shall be enabled by digital certification that allows secure Internet sessions to be established while conducting business with banks through JEPS applications. Digital certificates shall be stored on physical tokens. These tokens are personal. In the case of use of the public Internet, JEPS installations shall be protected by approved firewall systems.

11. Contractual agreements and obligations with third parties and banks

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

12. Business Continuity

It is important that procedures are in place to maintain the availability of an electronic payment system and the integrity of information being processed in the event of failure.

13. Business continuity and contingency planning

Business continuity planning is a corporate responsibility: each JEPS office (system administrators, users, managers) shall set up procedures to recover JEPS functions within three days. JEPS office shall carry out periodic risk assessments of the operational environment and perimeter security to ensure that all potential threats are recognized and resolved or adequate contingency measures documented and tested.

A risk assessment and local business continuity plan includes:

* Identifying internal and external threats and assessing the business risks arising from these threats (such as earthquake, civil war, power fluctuations)
* Determining the level of resources, performance and capacity requirements to maintain an JEPS service
* Identifying possible manual procedures that may temporarily substitute electronic systems.
* periodic testing, at least every six months, and continual review and appraisal of the plan to ensure that it remains current

14. Back-up and restore procedures

JEPS office shall be able to maintain transaction data on-line for a period of three months. Historical data may have to be maintained off-line for a period of one year. Operational data are usually maintained both at the receiving central bank and at the local JEPS levels. JEPS system shall be able to download from a central bank site at any time. In the case of local processing servers (i.e. when transactions are prepared

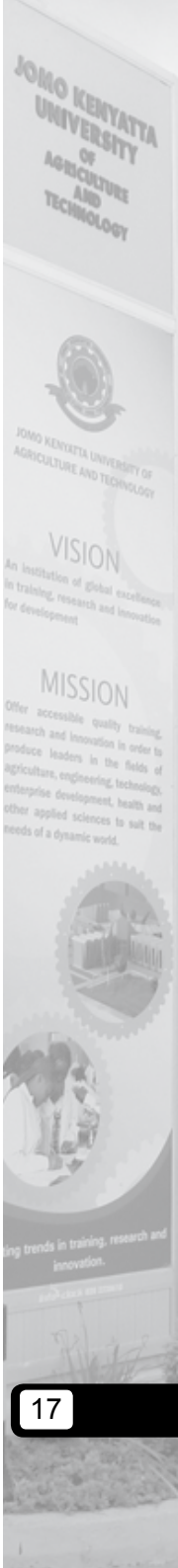
on site and then wired to central banks), users are responsible for and shall run back-up routines on a weekly basis. In the case of fully centralized systems (with no local storage of operational transactions) summary reports shall be printed daily and retained in order to provide recovery information.

As inputters, users managing daily operations with business data are responsible for their back-ups. Back-up media shall be adequately referenced, catalogued and securely held in sites that are physically removed from the JEPS location. When a back-up fails, inputters shall investigate the reasons and seek IT guidance, as necessary, to rectify the situation. A back-up log shall be generated as part of each back-up routine, including date and time of the back-up, data backed up, any error occurred. Back-up and operational restore/ recovery procedures shall be fully documented. Back-up media shall be tested regularly to ensure that they shall be relied upon for emergency use when necessary. Restoration procedures shall be regularly checked and tested to ensure that they remain effective and that continuity of service shall be maintained with minimal disruption. Data restoration shall be documented.

15. Installation and Change Control

1. System set-up

* The initial configuration of electronic payment systems shall be carried out by bank personnel in collaboration with JKUAT system administrators.
* Any initial configuration passwords required by the software on installation shall be immediately changed by JKUAT system administrators after set-up.



* All installation software is to be delivered unopened to a system administrator. It shall remain under his/her control at all times and be stored securely in a safe place both before and after the installation process, along with any configuration setting documentation.
* Any built-in account used by bank personnel shall be left in the JEPS system for support purposes only. This has to be formally requested by bank personnel.
* Clocks shall be set to local standard date/time and not changed; this is critical for the time stamp of business transactions, logs and user-ID authorizations.
* Full system configuration documentation recording the initial settings at installation shall be maintained.

2. Change control

Changes to electronic payment systems shall be controlled to minimize exposure to risks or failures. Change control includes but is not limited to:

* Equipment, such as back-up devices and printers
* JEPS computer operating systems
* Software and customized settings
* Physical security
* Configuration of connection lines and network security

A formal and documented change control process shall be used to restrict and approve changes to an JEPS.

All changes shall be authorized by a system owner and system administrators.

All software security fixes provided by banks or vendors shall be promptly installed.

Maintenance procedures shall be regulated by written instructions.

Where operational programs are changed, records have to be taken to identify the changes made, including before and after images.

To provide business continuity, in cases of major changes, a full back-up shall be made prior to any change in order to be able to restore previous conditions in the event of problems.

Following any change, the system documentation set shall be updated.

15.3 Control of Operations and Incidents

To ensure effective control and prevent errors or misuse, control of JEPS operations shall be carried out regularly. These controls cover operational activities such as payments and security areas. JEPS system shall provide audit logs, which contain the following events and details:

Operational logs

* Record of successful and rejected system access attempts
* Record of successful and rejected data
* Transmissions to banks and time stamps

Access logs

* User IDs with dates/times for log-on and log-off
* Terminal identification, including location, wherever possible

* Logging facility being de-activated

It is a system administrator's responsibility to effect a monthly review of:

* access rights
* physical security configuration
* logical security configuration
* status of equipment and JEPS software updates
* room access and line connection logs

It is an authorizer's responsibility to effect weekly control of transaction payments in order to identify 'out-of-pattern' activities and ensure that all rejected transactions have been rectified.

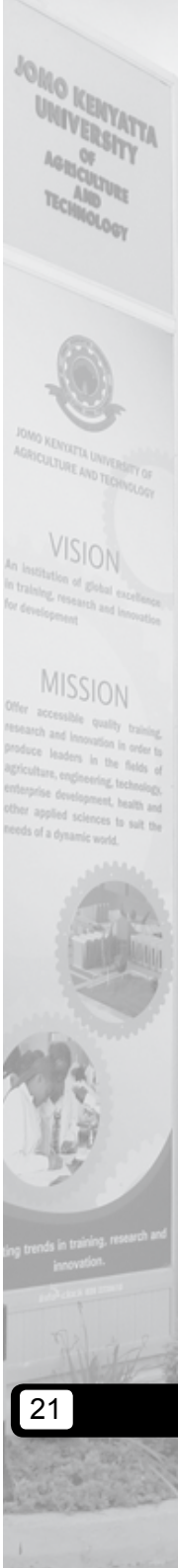
All users shall report any theft or loss of, or severe damage to, hardware or software; suspected compromises; and situations of serious security vulnerability.

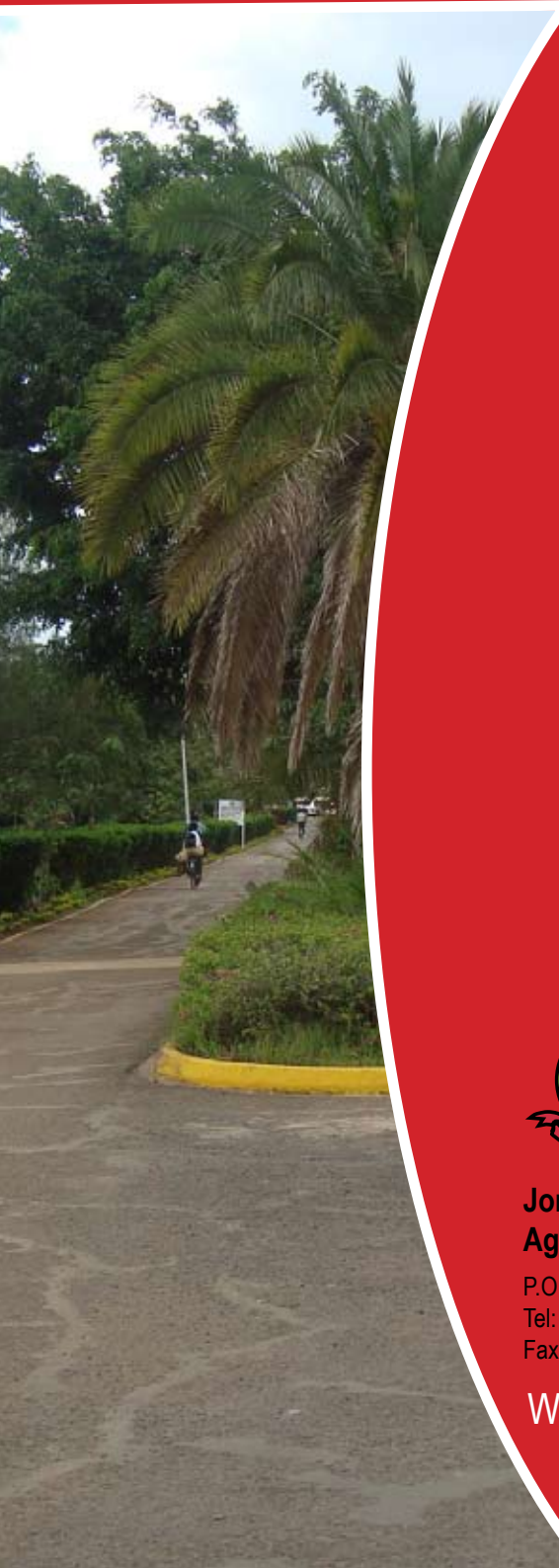
Staff with questions about information security shall contact the system administrator concerned.

In case of verified business or security incidents, these shall be reported to the system owner who, in accordance with the relevant offices and in collaboration with authorizers and system administrators, shall take the necessary countermeasures (such as payment cancellation, revocation of access, etc.) and/or inform the Office of Investigation, if deemed necessary.

4. Compensatory measures

In the case of small offices or evident limitations (such as outage of devices/lines for a limited time), when the security measures indicated in this document cannot be satisfied, compensatory controls shall be established. These are proposed by system administrators and formally authorized by the system owner.





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