POSTAL CORPORATION OF KENYA

SECURITY POLICY

Revision 3/2012

Preamble

Postal Corporation of Kenya security policy and related procedures provides guidelines for protecting both staff and customers, property and information at its disposal.The policy shall be used for security purposes as situations determine. To this cause, the policy remains a crucial document that help define the necessary security measures to be effected as situation demand.

Foreword

Protecting Postal Corporation of Kenya assets, employees, property & information is the responsibility of each and every employee in the Corporation. To assist in this effort, I am providing key managers with the attached Security Policy.

This Security Policy and Procedures are intended to establish the working relationships between management, staff, contractors and those partners and suppliers responsible for assisting the Corporation in protecting our assets from theft, loss, and risk. The Head of Security and Investigations shall provide PCK with support in dealing with emergency and crisis situations.

In managing our operations effectively, it is critical that the Corporation's funds, people, installations, equipment, ICT and environment be safeguarded or protected through sound management practices. We are showing, by the scope of the policy, our continued resolve to take effective management action and to highlight our responsibilities to protect our stakeholders' assets.

It is essential that each of you reviews own security requirements and develop an appropriate strategy. The Head of Security & Investigations will assist in the identification of security risks and in the development of appropriate strategies. He is also responsible for policy guidance and such protective functions as investigation, risk assessment and emergency operations.

This policy will be in effect throughout the Postal Corporation of Kenya premises and associated facilities and is to be used for your guidance in developing functional and facility security programmes that will comply with the overall Corporation policy. Please ensure that it is made available to and communicated to all staff in your department.

Dan Kagwe Dated……

Postmaster General

SECTION A

1.0 SECURITY STANDARDS

1.1. Perimeter Protection

1.1.1 *Objectives*

To protect against undesired intrusion into or exit from PCK's property. Such intrusion/ exit may lead to such incidents as sabotage, theft, industrial espionage or damage to PCK's facilities. This is also the first line of defence against civil violence. Whilst it may be practical to create an impregnable perimeter, the image factors often preclude this. With this in mind the goal is to obtain a degree of resistance efficient to deter the more "casual" intruder.

The perimeter must be homogeneous, i.e. no weak links at such areas such as the gates or breaks within the perimeter. In the event of a breach, an alarm system should alert the security staff, who would in turn co-ordinate and carry out an investigation or reaction.

1.1.2 *Standards*

Postal Corporation of Kenya standards require a wall or fence to be three (3) meters high. There should be no weak spots or climbing aids in the close vicinity of the perimeter. Damage or signs of intrusion or attempted intrusions should be repaired immediately.

The perimeter should be sufficiently well lit during darkness hours so as to enable routine security patrols to observe the area and identify intruders. The general lighting standards are:

i. Walls: Should be illuminated from above the over climb protection to the bottom. A strip inside the wall extending inwards for six to eight meters should also be lit to a minimum level of five lux.

ii. Buildings: They form part of the perimeter. They should be well lit to a depth of six to eight meters from the base of the building outwards and to a height of at least five meters above the ground level.

These standards are for areas where close circuit television is not in operation. Where close circuit television is used, appropriate lighting levels should be available to enable effective vision by means of the closed circuit system. Care should be taken to ensure that areas of deep shadow do not exist.

1.2 Access Control

1.2.1 *Objectives*

To protect against undesired intrusion onto the Corporation which could lead to sabotage, theft, espionage or damage to property.

Access control forms part of the first line of defence in that it will control all authorized openings within the perimeter. It is therefore necessary to identify who are entering, and the approval of any items that they bring with them. The identity of all persons wishing to

enter/visit the premises must be established. The degree of control must not be less than that of the rest of the perimeter.

Staff members are also encouraged to challenge people who do not have any form of identification and alert security immediately.

1.2.2 *Standards*

Postal Corporation of Kenya staff must be quickly identifiable in order to allow swift access through the barriers provided. This can be done either by physical examination of the staff identity cards by the Security Staff or preferably, by some form of automatic card reader system.

Recovery of staff ID cards from employees exiting PCK is paramount as is voiding an anti-pass back facility in the case of automated systems. Where automatic access control systems exist, all barriers should be slaved to that system and require the production of the appropriate staff ID cards to gain access to and egress from the premises.

The identity and bona fides of all other persons entering the Postal Corporation of Kenya or other terminal facilities must be established. This applies to such persons as casual labourers, interns, customers, contractors, suppliers and any other visitors. Each category of visitor may possibly require a different form of administration. This however must not transgress from the basic principal, that every person within the perimeter must have been authorized to enter at some stage or the other. A record with full details must be maintained in the hard cover book for quick reference.

Any property or items brought on site must be subjected to checks by security staff. The checks should be for items that could bring harm (weapons, explosives, drugs etc.) to the persons or property within the inside of the perimeter. Appropriate records should be maintained.

Where non - employees enter high security areas; they should be easily identifiable as being visitors to that area. A system should also be established to enable the easy identification of persons from one working area visiting another.

1.3 Egress Control

1.3.1 *Objective*

To protect against the unauthorized removal of the Postal Corporation of Kenya property from site.

1.3.2 *Standards*

The permit system should be enforced whereby relevant responsible person authorizes Corporation property being removed from Postal Corporation of Kenya or the terminal facilities. The permit shall be captured at the egress point and returned to the responsible person for verification of authority to remove the item and of the return of the item as may be applicable. Permits should be retained on file for a minimum of one year.

A search procedure should be enforced to identify undeclared corporation assets. In practical terms all obvious containers including private and official vehicles should be searched when leaving the Postal Corporation of Kenya. Where random searching suffices, a minimum ratio of one search per six exits would be appropriate. This should however vary from time to time.

Details of all vehicles, Lorries, Buses and customers' vehicles leaving the site should be logged, inclusive of items carried. Should rear-loading vehicles be in use, a seal system should be in operation and the number of seals recorded at the point of departure. These should subsequently be tallied with the seal numbers broken by the staff at the destinations. The seals should be held in a safe custody and be an accountable item.

1.4 Surveillance

1.4.1 *Objective*

To protect against the establishment and growth of organized crime by contracted staff, employees, customers and others, which may affect PCK's operations, profits, integrity and discipline

Management has not only the right but also the duty to discover such affairs actively through acceptable methods. Where liaison to other security agents, they should be exposed at the earliest possible opportunity to enable corrective action to be taken.

1.4.2 *Standards*

The gathering of information relating to the above must be done in such a manner so as not to jeopardize the image of the Corporation, industrial relations or place informants at risk.

Interviewing of information sources must be conducted in such a way that no undue attention is attracted. Information should not be directly utilized to discipline or prosecute individuals.

No covert technical aids should be used under normal circumstances. Where unaccountable losses or unresolved investigations have occurred, open surveillance by either human or electronic means can be introduced to observe activities, particularly in recurring trouble spots.

Routine and random patrols and visits should be conducted regularly both from a deterrent and a detection point of view. Routine patrols through selected risk areas should be at the maximum intervals of every two hours. A patrol should be operating within the premises twenty-four hours a day.

1.5 Processes/ Procedures and Training

1.5.1 *Objective*

To ensure maximum protection of Corporation assets, it is essential that all members of staff be guided by correctly laid down processes (and associated procedures) and be trained in those procedures to a high degree of competence. Amongst the areas that require

particular care are such subjects as inter-personal skills, interviewing and industrial relations. As members are constantly exposed to all sectors of staff and the public, it is imperative that they are fully conversant with their specific roles, duties and be well trained to carry out those with skill and discretion.

1.5.2 *Standards*

A complete set of Postal Corporation of Kenya procedures should be compiled, circulated and posted at each department / facility or uploaded in a share point portal for ease of access to any member of staff requiring making reference to them. They should be updated appropriately.

Other communication media should be fully utilized. This includes the use of the Occurrence Book, supervisor and subordinate meetings and small group briefs. Monthly reports should be submitted on an upward basis in a prescribed format from each region to the Head of Security & Investigations.

An annual training needs analysis should be conducted to identify individual skill gaps. These should be analysed and action taken to ensure that the training plan for the year is specifically designed to fill those particular needs. It is important that emphasis be placed on the gaps in the industrial and public relations area.

1.6 General Awareness

1.6.1 *Objective*

To protect against complacency or carelessness on the part of both management and the staff that could lead to unacceptable levels of risk management and key staff in high-risk areas should be required to contribute to the overall security program as an integrated effort. Further to this, they should be required to contribute satisfactory to security levels in their own areas of responsibility.

1.6.2 *Standards*

A close relationship should exist between the security management team and all other departments. Regular updates should take place to brief and update actions on actual incidents and potential problem area and threats.

An internal audit system should be enforced to highlight security weaknesses in high-risk areas to the responsible manager. Appropriate notices on boards and presentations/ educational programs for general staff should be conducted at least once per annum.

Induction of new employees into the Corporation should include critical aspects of security, safety and fire prevention.

The Postal Corporation of Kenya Security Committee should have a direct access to the Executive Management within the Corporation structure.

1.7 Information Protection

1.7.1 *Objective*

To protect against undesirable exposure of classified information. Corporation information shall be afforded protection commensurate with its nature and measures taken to safeguard information whose disclosure would be detrimental to Corporation interests. Employees shall not disclose to unauthorized persons Corporation information that is not already public knowledge.

1.7.2 *Standards*

A prescribed document classification system should be consistently enforced. This should cover the way classified documents are handled, and the lock up procedures that should be used and storage facilities to be provided.

Transmission, duplication and destruction practices must be carried out according to the laid down criteria.

A monitoring and reporting service must be provided to Management concerned.

1.8 Personnel Protection

1.8.1 *Objective*

To protect against harm or injury to key personnel by violent means as direct result of their occupation. The protection of human life is the primary objective of this Security Policy.

Human beings are the most valuable resources an organization can have; without them an organization cannot achieve its mission and critical objectives.

1.8.2 *Standards*

Any persons particularly those in key areas, who perceive or experience actual threats, should be interviewed in order to action a protective program. This should cover self-defence, emergency backup, minimization of self-exposure and irregular travel patterns. Home security in these cases should also be considered.

Persons normally working in high-risk situations (i.e. cashiers) should be inaccessible whilst carrying out their tasks. They should also have a facility to summon assistance rapidly. Some may require an armed protective officer or a strong cage with grills and ventilation.

1.9 Key Area Protection

1.9.1 *Objective*

To protect against risks of sabotage, arson, and theft in areas identified as top or high security. This security rating is applied to office of PMG/CEO, Cash office, office of Exchange, airports, ICT resources and equipment, which if disabled through any action would cause loss in operation continuity.

This is effectively a second line of defence against persons with ill-intent who have entered the site. Such persons are often grieving employees, contractors, casuals, customers or terrorists.

1.9.2 *Standards*

Postal Corporation of Kenya may contract security consultants that will be required to assess the above areas at each site and prescribe individual measures to harden and protect each facility. In areas where the hardening of assets has been completed, the general principals of actions laid down by the consultants should be utilized for daily area checks.

Excess of non-essential personnel in key areas should be restricted by physical barrier and door control. An entrance control system whether automated or manual should be introduced. An access control record should be maintained either by book or printout.

Where barriers are impractical, essential staff should be distinguishable from non-authorized persons. The use of coveralls or reflector jackets clearly marked with Corporation name should be introduced for identification purposes. A high degree of discipline in this regard is necessary. Full procedural access control in the form of a notification of the security department of discharges and any other means available should be strictly enforced.

Contractor staff required to work at PCK sites, must be cleared by security and the supervising department shall prepare a daily notification to security of the contractor working areas.

The AGM/Security & Investigations shall give a security brief to the contractor staff before commencement of work in all key areas.

1.10 Cash Protection

1.10.1 *Objective*

To protect against theft, loss or robbery of Corporation cash.

1.10.2 *Standards*

A survey of all cash collecting and holding points should be conducted quarterly to examine storage facilities, key holding responsibilities and accessibility. Recommendations should be submitted to the relevant departmental heads. Where possible, alarm facilities should be available to handlers, and intruder alarms provided both for offices and safes/ vaults. All cash must be secured in safes or strong room.

It is preferable that for cash in transit (CIT) contractor should undertake conveyance. Where this is not possible, physical security protection must be provided in liaison with Kenya police.

Cash balancing should be done on a daily basis to highlight at the earliest possible opportunity any discrepancies that may have come about as outlined in relevant accounting, financial and operational policies.

1.11 Fire Prevention and Protection

1.11.1 *Objective*

To protect against ignition and spread of fire, which would result in damages or destruction of property or corporation assets and death/ injury of staff.

1.11.2 *Standards*

The safety team should inspect the sighting and selection of fire-fighting equipment at least annually. Permanent equipment such as sprinklers and hydrants should be inspected half-yearly and serviced annually and portable equipment serviced as necessary. An efficient communications system to fire brigade should be in operation.

House-keeping inspections for fire hazards and non-smoking discipline should be carried out at quarterly. These should be followed by reports to the AGM Security & Investigations and Facility Management. Special attention should be paid to fire hazard area such as storage areas for inflammable materials or explosive substances. Quarterly inspections should be carried out to discover obstructed equipment and to ensure that sprinkler valves etc. are flushed correctly. A full log of all fire-fighting equipment, servicing and testing should be kept. Where fire alarms are fitted, they should be tested at least quarterly.

Fire-fighting teams on site (including all security staff) should be trained and practiced in their drills and the use of the equipment provided, on an annual basis. Motivation should be enhanced by the participation of teams in competition, external demonstration and the attendance at lectures. Correct protective clothing should be supplied.

2.0 EMERGENCY SITUATIONS

2.1 General

Terrorist attacks or threats, bomb threats, power failures, accidents to persons, fire, incidents affecting staff, demonstrations, water floods, etc. shall be considered as emergencies.

During all emergencies, the Head of Security & Investigations and Postal Corporation of Kenya management will issue the necessary orders as well as supervise measures to protect property and staff.

The security team at the facility is charged with the protection of property, personnel and they have an added task to assist in emergency situations.

An emergency list of the Crisis Management Team and telephone numbers is to be maintained in the security office.

2.1.1 Bomb Threats

In the event that a bomb threat is received, attempts should be made to keep the caller on the phone as long as possible, try to get the reason for the call, and ask the caller to repeat his message. Follow the bomb threat checklist attached to these instructions. Immediately on termination of the call, notify the AGM/ Security & Investigations or Security Officer present.

2.1.2 Explosive Devices

If a bomb or other unidentified device is discovered on premises, see to it that nobody touches or goes near the object. Evacuation of staff and any other persons in the premises should be immediately considered and the location sealed off. The police and emergency services are to be notified immediately.

2.1.3 Terrorist Threat

The threat from international terrorism has increased, notably since the 2001 September 11 (9/11) attacks in the United States of America. In this new environment, Postal Corporation of Kenya must also remain vigilant to such threats. Recent attacks by *Al Shabaab* clearly show that terrorists are prepared to attack the least well protected targets.

The threat of terrorism comes not only from established international groups, but also from cell-knit networks of individuals operating in Kenya and other neighbouring countries mainly Somalia.

The following simple preventative measures are to be observed:

2.1.3.1 Remain alert and vigilant. Keep an eye on suspect packages or vehicles, or people acting suspiciously, and report anything suspicious to the security office.

2.1.3.2 Trust your instincts; if you feel something is wrong, inform the security office immediately.

2.1.3.3 Terrorists seek other identities to protect themselves. Don't help them by leaving important ID documents e.g. passport, staff ID, driving licence etc.

2.1.4 Labour Disputes

The Head of Human Resources and Chief Executive Officer should be immediately notified if picketing, access blocking,etc., in regard to labour dispute is observed. Any unusual activities occurring in such situations should be noted. Additional security numbers may be deployed in cases where there is a likelihood of escalation.

2.1.5 Action in an Emergency

If an emergency occurs on Postal Corporation of Kenya premises; threats, explosion, damage to or destruction of property that may or results in injury or death of persons, the following action is to be taken by persons first at the scene:

2.1.5.1 Make immediate notification of occurrence to the security office.

2.1.5.2 Keep order, rope off the area, and render assistance to those in need

2.1.5.3 Assist in the care of the injured and evacuate from scene

2.1.5.4 The security guards are to restrict entry into the facility, allowing only the emergency services

2.1.5.5 The contracted security response team shall be dispatched to the scenequickly to secure the area and provide assistance

2.1.5.6 The security office is to reach the AGM/Security & Investigations and inform him of the occurrence

2.2 Letter and Parcel Explosives

2.2.1 *Introduction*

The purpose of this note is to provide guidance to members of staff, especially to those whose duties include Sorting, opening mail bags, etc on the identification of postal explosives and the measures to be taken should the necessity arise.

2.2.2 *General Aids to Identification*

2.2.2.1 *Form* - A postal bomb may be in the form of a letter, a package (e.g. a book) or a parcel. The first two forms are those most commonly encountered.

2.2.2.2 *Thickness* - A letter or book will almost certainly be thicker than an ordinary letter since it must contain explosive, detonator, battery etc. The overall dimensions of some of the devices encountered have been 180mm x 130mm x 12mm. Envelopes of such size may well be suspect.

2.2.2.3 *Envelopes (Private)* - Letter or book bombs are likely to be in plain

envelopes with ordinary postage stamps and addressed in manuscript.

2.2.2.4 *Envelopes (official)* - Mail sent between departments in official envelopes may be assumed to be safe but mail received from other sources neither should not be assumed to be safe solely by reason of the fact that it is enclosed in an official envelope.

2.2.2.5 *Addresses* - Care should be taken if an envelope is addressed to a senior official by either name or post. There is a possibility that names and titles of posts have been taken from a book of reference. Special attention should be given to mail addressed to persons who have ceased to hold the post attributed to them in the address given on the envelope.

2.2.2.6 *Mail received by messenger* - Letters, packages and parcels delivered by a person or a messenger who is positively recognized or identified maybe accepted as satisfactory. If the person or messenger is not immediately recognized or identifiable, his department, or firm should be contacted and proof of identify obtained. If there is still doubt the item should not be accepted.

2.3 Specific Aids to Identification

A letter, package or parcel should be treated as suspect if:

2.3.1 It comes from an unusual point of origin or sender; the postmark and/or name of the sender may, of course, be obscured and/or absent

2.3.2 The handwriting on the cover is of a style not usually encountered

2.3.3 It is lop-sided

2.3.4 Its weight seams excessive in relation to its size

2.3.5 There is any springiness in the top, bottom or side, but do not bend excessively

2.3.6 There are protruding wires

2.3.7 There is grease marks on the envelope or parcel wrapping or envelope

2.3.8 There is a smell of almonds or marzipan

2.3.9 The flap of the envelope is stuck down completely (usually there is an un-gummed gap of about 3mm, at the top of each side of the flap)

2.3.10 If it contains loose objects.

2.4 Additionally, in the case of a letter, it should be treated as suspect if:

2.4.1 It contains any form of stiffening e.g. by cardboard or metal, this can be ascertained by feel **but do not bend excessively**.

2.4.2 It weighs more than 50 grams and is more than 4.5mm thick; such a letter will need more than the usual value of postage stamps and will probably feel lopsided.

2.4.3 If, on opening an envelope, it is found to contain an additional envelope addressed personally to someone, this should be scrutinized again for signs of the characteristics listed above. An inner envelope, which is tightly taped or tied with string, should be treated as suspect.

2.5 Action

Persons who believe that they have received a postal bomb device MUST take the following actions:

2.5.1 ***Action in receipt of an item giving rise to suspicion***

2.5.1.1 Place the package on the nearest horizontal firm surface. Make no attempt to open it.

2.5.1.2 Leave the room, closing the door behind you. If it is possible to open the windows of the room before you leave, do so. Prevent other persons going into the room. Lock the door if possible.

2.5.1.3 Inform the Security Office or Supervisor immediately.

2.5.2 ***Action if suspicions are aroused after a package has been partly opened or the contents removed.***

2.5.2.1 Order any other staff present to leave the room as quickly as possible

2.5.2.2 Place the package or the contents of the package (as the case may be) as gently as possible on the nearest horizontal firm surface keeping the face and body shielded e.g. by placing the suspect item behind a substantial object such as steel cupboard.

2.5.2.3 Leave the room quickly closing the door, prevent other persons going into the room and lock the door if possible.

2.5.2.3 Notify the Security or supervisor immediately.

2.5.2.4 On no account should a suspect item be:

i. Removed from the room.
ii. Placed in a bucket of water.
iii. Covered with sand

3.0 SECURITY COMMITTEE

3.1 ***Purpose***

3.1.1 The Postal Corporation Security Committee is established to assist the management in the implementation of the security policy. The Chief Executive Officer to whom they will be responsible for providing overall policy direction relating to all security matters will appoint the members of the committee.

3.1.2 The Security Committee will transform itself into a Crisis Management Team (CMT) in the event of a security crisis.

3.1.3 The Security Committee will hold meetings on a monthly basis.

3.1.4 The Head of Security &Investigations will act as the secretary to such meetings and will ensure that minutes of every meeting are produced and circulated to all members or stakeholders.

3.2 ***Membership***

3.2.1 The membership to the Security Committee will be as per the Crisis Management Team.

3.3 ***Responsibilities***

3.3.1 Monitoring the type and changing levels of threat to Postal Corporation of Kenya interests.

3.3.2 Identifying additions and other amendments necessary to Postal Corporation of Kenya Security Policy to meet changing security needs.

3.3.4 Providing advice on the appropriate means of implementing Postal Corporation of Kenya security policy to all areas and associated facilities.

3.3.5 Receiving and examining reports submitted to the Chief Executive Officer following security incidents.

3.3.6 Arranging security audit checks to be done at selected locations, as decided by the Chief Executive Officer; analysing the reports subsequently submitted by the audit team.

4.0 CRISIS MANAGEMENT TEAM

4.1 Purpose

4.1.1 To protect against unpreparedness or breakdown of management control in the event of an emergency situation arising from such threats as terrorist attack, bomb, riots, strike, explosion or fire.

4.1.2 To limit the impact from disaster through calm and coordinated reaction. It is necessary to ensure all staff, particularly key personnel are aware of their roles in crisis management. It is distinct from contingency planning, which encompasses the use of alternate resources for the continuance of or production and distribution services.

4.2 Standards

4.2.1 Contingency plans should be prepared, circulated and practiced to deal with the evacuation or lock in as may be indicated by the situation. At least one practice should be carried out annually. Assembly points must be suitably sited and marked.

4.2.2 Exit routes should be marked and unobstructed. Where possible emergency lighting or luminous directional lighting should be provided.

4.2.3 Plans should cover both working hours and after hour possibilities. The contingency plans should aim:

4.3 Objective

4.3.1 To ensure that the security needs of Postal Corporation of Kenya and other facilities is not compromised.

4.3.2 To provide operational continuity.

4.3.3 To minimize any disruptions to Postal Corporation of Kenya or facility operations.

4.3.4 To resolve the emergency/crisis as quickly as possible.

4.3.5 To ensure protection of life and property.

4.4 Roles and Responsibilities

The roles of key personnel should be clearly defined and available to them. An effective communications system should be at their disposal for crisis control. To facilitate the same, the following is necessary:

4.4.1 An emergency control room must be designated and suitably equipped.

4.4.2 Bomb threat procedure as well as standard mail opening precautions, search policy and like procedures should be laid down.

4.4.3 Links with emergency authorities, bomb squad, riot squad and the police should be available to allow medium communication with these authorities. Routine communications with these agencies should be on a familiarity basis.

4.4.4 Local evacuation alarm must be audible to all areas.

4.5 Procedures

Emergency Procedures and immediate actions to be taken in the event of an emergency include the following:

4.5.1 The Risk Management Team (Compliance) will carry out a quick threat assessment of the crisis

4.5.2 All Postal Corporation of Kenya key staff will be alerted of the looming crisis

4.5.3 The Crisis Management Team members will be notified to assemble by the Head of Security & Investigations, giving time and place for the meeting

4.5.4 Dependent on the scale of the crisis, the emergency and security agencies will be alerted.

4.5.5 Monitoring teams will be dispatched to crisis locations immediately.

4.6 Composition of Crisis Management Team (CMT)

The Crisis Management Team will be composed of individuals who would essentially be responsible for the overall coordination and direction of all activities.

4.7 CMT Assembly Point

The CMT members will assemble at the Posta House Boardroom and hold their deliberations in a secured environment or any point that shall be suitable for meetings.

4.8 Communications

All CMT members will be reachable through their cell phones. The Risk Management Team will move with speed and ensure communications centre is set up and available for the CMT members, at scene of crisis and for the monitoring teams.

4.9 Monitoring Teams

In an event of a crisis, the team is dispatched immediately to scene. The purpose is to keep the CMT informed on events as they develop. The CMT will be composed of specialized individuals drawn from security and relevant department(s).Initial Response CMT

Immediately the CMT has been assembled, they will quickly prepare and plan for the following:

4.9.1 Access control into and out of all locations.

4.9.2 Protect critical security areas, may consider evacuation of location.

4.9.3 Liaison with Police and other emergency services representatives.

4.9.4 Plan and execute a recovery action.

4.9.5 Assessment of liabilities arising from crisis.

4.9.6 Provide advice on required actions to be taken to Postal Corporation of Kenya management.

4.9.7 Reassure key customers

4.9.8 Establish contact with other companies in the close vicinity and coordinate actions.

4.10 Incident Reporting

4.10.1 ***General***

To ensure a coordinated approach for the receipt and dissemination of information on all incidents and threats targeting the Postal Corporation of Kenya facilities.

4.10.2 ***Standards***

4.10.3 Security Reports should include the following;

- 4.10.3.1 Correct time and date
- 4.10.3.2 Exact location of occurrence and location of persons, vehicles and objects involved
- 4.10.3.3 Complete names and identification numbers of involved staff.
- 4.10.3.4 Complete names and identification numbers of witnesses.
- 4.10.3.5 Detailed description of events.
- 4.10.3.6 Security staff involved or investigating.
- 4.10.3.7 Disposition of the incident.
- 4.10.3.8 Were emergency services notified?
- 4.10.3.9 Time of arrival of emergency services
- 4.10.3.10 Actions taken
- 4.10.3.11 Injuries or property damage involved

4.11.4 Reports are to be submitted in the following instances;

- 4.11.4.1 Any robbery, intrusion or alarm activation.
- 4.11.4.2 Any dishonest or criminal activity or other violation of Postal Corporation of Kenya regulations within sight or hearing.
- 4.11.4.3 Any emergency situation concerning existing or threatened espionage, sabotage, and subversive activities, as well as loss, compromise or suspected compromise of sensitive material.
- 4.11.4.5 Any terrorist threat, bomb threat or explosion.
- 4.11.4.6 Accidents that involve injuries to staff or visitors on premises etc.

SECTION B

OPERATING PROCEDURES

SECURITY STANDARD OPERATING PROCEDURES

This section of the document contains the procedures, which describe and detail the implementation of the security policy.

The key procedure is "Security Management Plan" which provides a simple guide to the implementation of all other procedures and should be very well understood by all staff and in particular those with security responsibility. For each of the major aspects in the life cycle of a given operation it identifies which procedures should be utilized or consulted.

The procedures as outlined in this document are intended to be practical and applicable in any and all of the situations and locations of POSTAL CORPORATION OF KENYA operations. The document is self-contained so that each HOD with only this document will be able to establish and implement a security function consistent with POSTAL CORPORATION OF KENYA objectives and standards.

This edition of the document was issued in ---------- (date) by the Head of Security & Investigations and must not be changed without his authority. Revision numbers will identify subsequent revisions and updates and issue dates as appropriate. It is the responsibility of the relevant HOD to establish a system for the control and maintenance of subsequent updates to the document.

Note that this document contains potentially confidential data and should be controlled accordingly. Should there be any concerns or queries regarding the contents or interpretation of this document they should be addressed to:

Maj. (Rtd) A. T. M. Lumadede
TEAM LEADER – SECURITY & INVESTIGATIONS

SECTION B

STANDARD OPERATING PROCEDURES

5.0 ACCESS CONTROL PROCEDURES

Sound access control procedures are the cornerstone of building and maintaining an effective security programme. It is, therefore, necessary to establish a standard for access control that will be applied at the various Postal Corporation of Kenya facilities assuring that only persons on legitimate business are admitted thus making it easier to detect and preclude someone who should not have access.

Security Staff shall;

5.1.1 Ensure that no unauthorized persons or vehicles gain access to PCK's premises.

5.1.2 Ensure that no employee or an employee of a contractor, or any vehicles exits official premises in an irregular manner.

5.1.3 Ensure that all visitors are courteously received, assisted and directed in a manner which will reflect PCK's credit; to record, as directed, such details of visitors and vehicles that are authorized to access official premises.

5.1.4 Record all vehicles visiting PCK premises to collect or deliver items; and issue relevant gate passes.

5.1.5 Implement PCK's RIGHT of search of employees, visitors and contractors including their vehicles to ensure that official property is not taken off the premises without due authority.

5.1.6 Require the production of authorization for the removal of Corporation property including borrowed tools to record and deal with those authorizations in accordance with practice.

5.2 STAFF ACCESS

All staff will be issued with standardized official photo identification cards for the following purposes:

5.2.1 Identification at all Postal Corporation of Kenya facilities
5.2.2 Card reader access admittance at controlled doors where they are in use.

The following procedures apply to the use of ID cards to enter Postal Corporation of Kenya facilities:

5.2.3 The Security Staff will check staff ID cards at the point of entry on a random basis to ensure identification cards are still in the possession of the staff and that the staffs have their own ID card.

Forgotten or lost staff ID Cards;

5.2.4 Where the staff is not known to the in-charge of Security and has forgotten his/her staff ID card, some positive identification must be produced such as a National ID card, passport, etc.

5.2.5 The in-charge of security shall verify the staff status to ensure that s/he is a current employee of PCK.

5.2.6 A temporary staff ID card shall be issued at the security office on exchange with a National ID. The staff will be advised that he/she must return the temporary staff ID card upon leaving the Postal Corporation of Kenya or facility.

5.2.7 Where the staff ID card is lost, the employee shall inform the Head of Security & Investigations in writing through his/her Controlling Officer.

5.2.8 The staff shall be required to report the loss to the Police and obtain the relevant Police Abstract which shall be presented to the Security Office to facilitate issuance of a temporary staff ID card while awaiting issuance of the replacement.

Termination of service

5.2.9 Where an employee exists the services of PCK, s/he will be required to surrender the staff ID card to security & investigations office upon clearance from service.

After Hours Access

5.2.10 When PCK's facilities are officially closed, all staff entering the premises to conduct business must submit written authority duly signed by their respective HOD.

5.2.11 The authorised employee should sign in the relevant logbook/register at the entry point and sign out on exit.

5.2.12 The Security Officer in charge of the premises will implement the Corporation's right of search of employees and contractors and their vehicles in order to ensure that Corporation property is not taken from the premises without authority.

5.3 CONTRACTORS

These are non-Postal Corporation of Kenya personnel who may require intermittent and continuing access into Postal Corporation of Kenya and other facilities to perform work under a Contract. Such works will generally consist of installation, repairs or maintenance to machinery and equipment.

5.3.1 Information regarding the contractor's name, address, the type of contract work and the areas where the work is to be done will be furnished by the HoD of the user department and/ or procuring office concerned to PCK's Head of Security & Investigations at least five (5) days before commencement of the works.

5.3.2 Contractors shall furnish the Security Office with a list of their personnel who will be performing the contracted works indicating their national identity card and telephone numbers.

5.3.3 All contract personnel shall have acceptable company identification cards to facilitate processing of gate passes and must register at the access point and sign out upon exit.

5.3.4 PCK shall not be responsible for safeguarding contractor tools or equipment while at official premises.

5.4 VEHICLE ACCESS

5.4.1 All vehicles entering PCK premises shall be recorded at the access point by vehicle registration number, driver particulars (name & ID) and entry & exit times recorded.

5.4.2 All vehicles shall be required to observe the stipulated speed limits and parking designated slots as guided.

5.4.3 Commercial vehicles i.e. carrier trucks, delivering mails or materials, contractors and suppliers shall be subjected to inspection and security checks upon access and exit.

5.4.4 Vehicles exiting with PCK property shall be required to possess a valid and authenticated removal document/gate pass.

5.4.5 All unattended vehicles shall be parked and locked securely at the designated parking bay.

5.4.6 All vehicles parked should be free from liquor, arms, weapons and other dangerous weapons.

5.4.7 Any external driver or staff who floats PCK's motor vehicle movement regulations shall be restricted/ or denied access to official premises even if one had enjoyed these rights previously.

5.4.8 PCK shall not take responsibility of the security of vehicles parked at its premises.

5.5 VISITOR ACCESS

5.5.1 Visitors shall be permitted within the normal office hours during official working days and no visitors shall be allowed outside the stated duration unless with the express permission of the respective HOD.

5.5.2 All visitors shall register at the reception by name, ID No and telephone number and be issued with a visitor's badge which should be conspicuously displayed by the visitor while in PCK premises and surrendered back on exit.

5.5.3 The visitors details shall be maintained in the log register for a period of at least one year and the register shall be checked periodically and at random by the Head of Security & Safety to ensure adherence to proper registration procedures.

5.5.4 Each PCK facility shall have one designated visitor control point and it is preferable that visitors are attended to at a designated place unless it is a business visitor who shall be guided/escorted appropriately to the host.

5.5.6 Under no circumstances shall visitors and unauthorized personnel be allowed to classified highly sensitive and security risk areas such as strong rooms, registries, ICT, sorting offices, etc.

5.6 VIP VISITS

5.6.1 The hosting HOD or delegated representative shall inform Security Office of the intended VIP visit giving the relevant details i.e. visitor's name, arrival date & time.

5.6.2 Upon arrival, the Security Officer shall receive the visitor, issue the visitor the relevant visitor badge and escort him/her to the host or meeting room.

5.7 OFFICE SECURITY GUIDELINES

Office security is very important, more so than most employees realise. In general employees who work in offices become complacent about the documents or keys they are handling which in turn can lead to breaches of security. Documents, which are in use, are often left in open view on desks and in trays even when offices have been vacated for breaks.

Offices, which handle sensitive or confidential documents should never, be left unlocked, when empty unless all documents are secured in a metal cabinet with a good lock. It takes a very short period of time to either make a copy or remember roughly the contents of a sheet of A4. Similarly keys must be signed for from the security office and returned at the close of the day.

Subsequently, all employees shall adhere to the following office security guidelines;

5.7.1 The office door should be locked when not in use at night, weekends or holidays or when it is left empty for more than a few minutes through the day:

5.7.2 At night, weekends and public holidays office windows should be secured priorto locking the office:

5.7.3 Personnel should not leave keys to their offices in the office drawer:

5.7.4 Unescorted visitors, including workmen, should not be allowed admittance without proper identification and authorisation and should not be left on their own in the office:

5.7.5 Papers and documents of a confidential nature should not be left exposed on desk tops, in trays, filling cabinets or other office furniture:

5.7.6 Janitorial and maintenance activities in key offices should be supervised by a competent employee:

5.7.7 Staff should be alert to strangers in the office complex, if unsure they should ask the person who they wish to see and what they are doing. If there is still some doubt, report to the security office immediately:

5.7.8 When answering phone calls do not divulge whereabouts, names, addresses or telephone numbers of members of staff. As a standard policy take a number where the caller can be contacted then pass it on to the person who was enquired about:

5.7.9 Keep travel itineraries confidential. Limit distribution to those who need to know:
Do not tempt thieves by leaving valuables or money unsecured:

5.7.10 If sharing an office or group of offices stagger lunch hours and coffee breaks so that the office is occupied at all times during the working day:

5.7.11 Arrange office furniture so that anyone entering the office can be seen easily:

5.7.12 Do not label keys in plain English, use a form of code then if it gets lost it will not be easily identified.

5.7.13 Do not leave keys under flowerpots, calendars etc. Thieves know all the hiding places!

5.8 Key Security

All departments within the Postal Corporation of Kenya should hold a list of keys, their function and who are the authorised holders within that department. Facilities department should also hold a copy of the same for each department. The Departmental Head of those who require access to the keys held in the gatehouse should forward a list to the Head of Security & Investigations.

5.9 Lost Keys

5.9.1 Any lost or misplaced keys must be reported to the head of the relevant department immediately in order that locks can be changed if required.

5.9.2 If the loss of any key means those assets will be vulnerable until the lock is changed then the security section should be informed so that guards may be posted to protect those assets.

5.9.3 Prior to any locksmith being employed on site, his/her name and company details should be forwarded to the Head of Security & Investigations so that checks can be made to reduce the risk of a problems occurring at a later date.

5.10 Corporation Safes

5.10.1 Only those authorized employees who need to know should know the number and locations of respective safes.

5.10.2 Only those authorized employees who need to know should know the location of the safe keys, spare keys and key holders.

5.10.3 All safes or cabinets fitted with a combination lock should be reset at irregular intervals but after a period of time not more than three months.

5.10.4 Should there be any compromise of the integrity of a safe lock or cabinets, which contain sensitive items or money, the lock should immediately be reset or replaced.

5.11 Security of Sensitive Items

5.11.1 Restricted, confidential or sensitive documents, computer disks or other such items as cash should be secured in corporation safes or security cabinets.

5.11.2 The security of personal documents and other valuable items are the responsibility of the owner and should be kept under lock and key when not in use.

5.12 Destruction/disposal of sensitive documents

The destruction of sensitive documents is important and if any member of Postal Corporation of Kenya staff is unsure of what to do with documents for disposal they should refer to the originator or holder of the papers to be disposed off in line with the stipulated conditions regarding disposal of the subject document.

5.13 Telephone Security

The telephone system is far from secure and is in fact a very easy means of communication to listen in to should someone wish to do so. All staff should therefore bear in mind that everything they say over the telephone could be heard and could be recorded by someone else. With this in mind it is important for the security of individuals and of corporation information that items of a confidential or sensitive nature should not be discussed over the phone. As little as possible should be mentioned with regard to future movement of staff, future operations or anything, which might be of interest to rival operators.

6.0 CORPORATION VEHICLE SECURITY

PCK vehicle security shall be as implemented as stipulated in the relevant Fleet Policy that is in force.

7.0 SECURITY SURVEYS

A security survey is an extremely important and useful document. It examines virtually all aspects of a security programme. Essentially, it is a critical, detailed examination and analysis of an asset (building or personnel) in order to ascertain the current level of security, identify deficiencies or excesses, determine the level of protection required and provide recommendations to improve the security of the examined asset. The security survey presents a total picture of the existing security programme that includes, but is not limited to, physical security, access control, communications, contingency planning, and local guards. When completed, a security survey becomes the official or primary record of the overall security programme at the duty station and provides invaluable information for developing or updating the corporation's security plan.

Under normal conditions, a security survey shall be conducted once every twelve (12) months. However, the security situation may dictate updating more frequently. In any event, after the initial survey has been conducted, it is useful to review it for accuracy on a yearly basis.

Security surveys will be coordinated by the Head of Security & Investigations.

8.0 CONTRACTED SECURITY GUARD OPERATING PROCEDURES

8.1 Introduction

These procedures for the contracted security firm are part of the overall Security Policy for Postal Corporation of Kenya and will be reviewed constantly and amended where necessary to ensure that the procedures provide an up to date system from which the security operations can be effectively applied. In order that the security of PCK personnel and assets remains at a high standard it is important that the contracted security staff follow these rules and fulfil their role to the best of their abilities at all times.

8.2 General

The primary responsibility of the contracted security is the protection of PCK staff, premises, property, vehicles and products. Whilst carrying out their duties the security staff must conform to the following at all times:

8.2.1 The security staff shall be correctly dressed and presentable at all times and must remain alert, vigilant and be courteous always, regardless of the situation they are confronted with.

8.2.2 Whilst on duty the security staff will not sleep nor will they allow themselves to engage in any activity, which might distract them from carrying out their duties in a professional and efficient manner.

8.2.3 Batons, clubs, night sticks or any other object carried by the guard may ONLY be used in self-defence should they be attacked and not to aid an arrest if an intruder or member of staff is caught carrying out an offence against PCK property.

8.2.4 Should it be necessary to use physical force to carry out a *citizen arrest* to prevent theft or damage to the corporation's assets or to prevent injury to staff, only the MINIMUM use of force as permissible by Law shall be allowed.

8.3 Tour of Duty/ Changing of Guard

8.3.1 The tour of duty for security staff will be as per the SOPs prepared by the contracted security management in line with the performance contract and conforming to the relevant labour laws. The recommended periods of watch are to be divided into two:

- Day Shift - 06:00 A.M. to 06:00 P.M.
- Night Shift - 06:00 P.M. to 06:00 A.M.

8.3.2 Security guards will only leave their posts after they have been relieved by the incoming guard.

8.3.3 Security guards not on duty will not be allowed to remain on PCK premises after they have been relieved of duty and shall be required to leave the facility immediately.

8.4 Standing Orders

All contracted staff must be conversant with PCK security instructions as issued from time to time. The contracted security management will write appropriate Security Standing Orders and Procedures for each post manned.

8.5 Discipline

8.4.1 As the first point of contact, they are to receive PCKstaff and visitors at the entry points and should treat them with courtesy, however, should be firm and fair on security & safety maters.

8.4.2 The on-site Security Supervisor is responsible for the efficiency of the security staff deployed at all locations. Staff on security duties will be supervised at intervals of at least two hours.

8.4.3 Any discipline matters that have a direct impact on PCK security shall be reported to the location PCK Security Officer without delay.

8.5 Reporting and Contact

The contracted security supervisor on site at the HQs is directly responsible to the AM/Security & Safety while those stationed at the regions shall report to the respective RSIO on the day-to-day operations.

8.6 Responsibilities

The contracted security firm is responsible for the physical security of all POSTAL CORPORATION OF KENYA property, facilities, assets, products and staff. They are to ensure that correct procedures as detailed in these orders, in relation to the logging of vehicle movement, visitors and the searching of vehicles are adhered to.

8.7 Equipment

The security guards must be equipped with all necessary gear for the smooth and efficient performance of their duties. These will include a standard whistle, remote panic button, torch and baton.

8.8 Dress code

The security guards shall be required to wear smart and clean uniforms at all times whilst on duty. They should be provided with boots, belt, cap and jackets by the contracted security firms.

8.9 Identification

The guards shall be required to carry and display their staff identification cards to ensure they are quickly identified as guards belonging to the contracted firm.

8.10 Guarding duties

The duties of the security guards within POSTAL CORPORATION OF KENYA facilities will be:

8.10.1 Prevention of illegal removal of PCK assets, goods and property from PCK facilities.

8.10.2 Protection of Corporation premises and other property from malicious damage and or sabotage.

8.10.3 Prevention of entry into PCKpremises/facilities by unauthorized persons

8.10 Access Control

Only AUTHORIZED PCK staff, visitors and contractors shall be permitted to access PCK premises and facilities. In order to ensure that only authorised personnel are permitted to enter, it is important that all staff wear their staff ID passes at all times while on the site. The security department with help from the contracted guards shall ensure the following:

8.10.1 Security staff shall check all passes of those wishing to enter PCK premises and all other facilities regardless of their position within the Corporation.

8.10.2 All visiting PCK personnel shall also to be checked and must display their security passes.

8.10.3 All visitors who need access to PCK premises and other facilities shall be issued with a visitors pass.

8.10.4 The access gates are to remain closed during the daytime and must be locked at night except when they are in use.

8.11 Security Patrols

Patrolling must be carried out constantly both day and night to act as a deterrent and to keep watch over the site and assets inside it. Guards should not be focussed only on what goes on inside but must be watchful of the area outside the fence as this may provide early warning of a criminal activity.

8.11.1 Whilst guards are patrolling they are to remain constantly alert and suspicious to the threat of intruders trying to gain access to the PCK or other facilities.

8.11.2 Guards must constantly be on the lookout for anyone attempting to, or in the action of stealing, damaging or otherwise tampering with property, which they are not, authorised to take or to tamper with. Particular attention is to be paid to the following whilst guards are patrolling:

- 8.11.2.1 The perimeter fence and the ground both immediately inside and outside
- 8.11.2.2 Parked vehicles
- 8.11.2.3 That all doors that should be are locked and that padlocks are not broken.

8.12 Security Searches

Random searches shall be made on both personnel and vehicles when they exit PCK facilities. Guards shall ensure that:

8.12.1 All personnel and vehicles exiting official premises shall be searched including those in senior management positions.

8.12.2 Searches shall be carried out in a professional, logical and systematic manner courteously but firmly.

8.12.3 Female members of staff and visitors shall be searched only by another female and out of sight of public view while the same shall be applied to male personnel.

8.12.4 Anyone who declines/refuses to be searched or uses abusive or threatening language or behaviour towards the security personnel shall bereported to the PCK locational Security Officer immediately to enable him/her address the situation.

8.13 Key Control

All keys kept in the Security Office for safe keeping are to remain in the key cabinet under key & lock at all times until required for issue. The cabinet is to be locked unless it is required for use and the key for the cabinet is to remain with a responsible security officer staff.

8.13.1 Only those persons authorised to sign out a particular key or keys shall be permitted to do so.

8.13.2 A list of those authorised persons shall be held in the Security Office and will be updated at regular intervals as need arises.

8.13.3 Issuance and return of all keys shall be logged in the relevant book.

8.13.4 The loss of any key or keys is to be logged and reported in writing to the relevant Controlling Officer and the locational PCK Security Officer.

8.13.5 Should any property, vehicles or assets be exposed to any risk as a result of the loss of a key, security must be maintained until such time as a replacement lock can be arranged and fitted.The relevant RPM and Head of Security & Investigations must be informed immediately.

SECTION C

INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICIES

TABLE OF CONTENTS

I. STRUCTURE OF THE DOCUMENT

This document contains the Information Security (Part A) and Information Technology Security Policies (Part B) for Postal Corporation of Kenya. The policies form the high-level requirements necessary to achieve PCK's information security objectives, and are guided by relevant regulations and standards, security industry best practices and control requirements specific to PCK'soperating environment.

These policies have been closely aligned with industry standard, ISO 27001ICT Security and Policy Section. This standard has emerged as the leading best practice guidance for managing information security within an organisation, and provides a framework for the process of ensuring information security. The designated security objectives are intended to provide compliance coverage for:

- Data protection and privacy laws
- Personal Identifiable Information (PII)

Statements containing:

- a '**must**' are mandatory requirements.
- a '**should**' are best practice specifications, where compliance is generally expected unless a significant business reason exists to the contrary.
- a '**will**' refers to actions that are part of an existing process, e.g., "users **will** be subject to disciplinary action" or "variances from policy **will** be dealt with on a case-by-case basis".
- a '**may**' refers to an open option for decision, e.g., "Administrators **may** be required to provide strong passwords before inbound access to system administration console can be permitted, if requested by the Security Team."

II. PURPOSE AND SCOPE

1.1 Definition and Purpose

The central and critical role of information and information systems at Postal Corporation of Kenya underscores the importance of ensuring the protection of these systems. The availability, accuracy, integrity and confidentiality of PCK information systems are essential to the organisation and to our relationships with consumers, providers, business partners, other government agencies and employees. The data stored on our systems, as well as the specialized software programs and systems developed for our use, are extremely valuable assets and must be protected. This Information Security Policy outlines, at a high level, the responsibilities and expectations for security of the information assets managed by PCK.

The purpose of this Information Security Policy document is to clarify the policy expectations for the IT environment for both its managers and users. These expectations have been produced from an analysis of standards for ICT Security and Policy Section, from security "best practices", from requirements mandated by the government and through consensus within the PCK. This document is subject to

periodic review, particularly considering the evolving technologies, regulatory or industry demands and business requirements.

The Information Security Policy establishes a security program designed to:

- Reflect the Postal Corporation of Kenya objectives.
- Prevent the unauthorized use of or access to information systems.
- Maintain the confidentiality, integrity and availability of information.

1.2 Scope

This Policy describes the security program for both online (in a machine-readable format) and offline (on paper or other media) information.

This policy applies to all computer and network systems owned by and/or administered by Postal Corporation of Kenya, and to any systems administered or managed by third parties for and on behalf of the Postal Corporation of Kenya.

The policy includes all computer types (terminal servers, database servers, web servers, ftp servers, storage systems, local area network file servers, personal computers, network equipment, telecommunications systems, and peripherals), operating systems and application systems, whether developed in-house or purchased from third parties.

Although the audience for this Policy and supporting documents referenced is primarily employees, its principles and requirements apply to all users of within the Postal Corporation of Kenya information systems and applications. This includes consultants, contractors, temporary workers, business partners, members, providers and others who access or use the Postal Corporation of Kenya information systems. Targeted guidance for specific audiences may be created as necessary in order to communicate aspects of the security program to *parties* external to Postal Corporation of Kenya.

Users who deliberately violate this or related information security policy statements will be subject to disciplinary action up to and including termination of employment, legal ramifications, removal of access or any association with Postal Corporation of Kenya.

1.3 Variance

Postal Corporation of Kenya requires that information security be maintained at all times. However, situations may arise that cannot be effectively addressed within the constraints of existing information security policies and standards. To provide for a standard way of identifying and tracking controls that are not in compliance, ICT Security and Policy Section provides a process for reviewing, approving or denying and tracking requests for variances.

All variances to the Information Security Policies and Standards are to be requested in writing to the Asst. General Manager of ICT and the IT Security& Policy Unit. Requests must be approved

before proceeding. Deviations from information security policies and standards are prohibited without prior written approval. Each variance request evaluation will take into account the compensating benefits to the Postal Corporation of Kenya. Requests that create significant risks without compensating controls will not be approved.

III. ROLES AND RESPONSIBILITIES

1.4 Data Owners

Data owners are senior organisation unit managers with the authority to acquire, create, and maintain information systems within their assigned area of control. Owners are responsible for categorising the information for which they have been designated as an Owner using the classifications defined within the *Information Classification Standards*. To assist with contingency planning efforts, Owners are also responsible for categorizing information (or specific application systems) according to the criticality defined by ICT Security and Policy Section. Owners are additionally responsible for authorising user access to information, based on the need to know. Owners must also make decisions about the permissible use of information. Owners are furthermore responsible for establishing relevant controls for information consistent with policies and standards issued by ICT Security and Policy Section. Separately, Owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labelling, and other security related control deficiencies pertaining to the information for which they are the designated owner.

1.5 Data Custodians

Data Custodians are technical contacts that have operational-level responsibility for the capture, maintenance and dissemination of a specific segment of information, including the installation, maintenance and operation of computer hardware and software platforms. Data Custodians may or may not be IT staff. Data Custodians will:

1. Define and implement processes for assigning User access, revoking User access privileges, and setting file protection parameters.
2. Implement data protection and access controls conforming to the Postal Corporation of Kenya *Information Communication Technology Policy*.
3. Define and implement procedures for backup and recovery of information.
4. Ensure processes are in place for the detection of security violations.
5. Monitor compliance with the *Information Security Policies and Standards*.
6. Limit physical access to information assets, including:
    a. Equipment control (inventory and maintenance records), and physical security of equipment.
    b. Authorisation procedures prior to physical access to restricted areas, such as data-centres, with sign-in or escort of visitors, as appropriate.
7. Implement a system for software change management and revision controls.

8. Maintain on-going internal audit processes (to the extent technologically practical), which record system activity such as log-ins, file accesses, and security incidents.
9. Maintain records of those granted physical access to restricted areas.
10. Provide special handling and physical protection for assets, including:
    a. Operating and maintenance personnel are given access only as necessary to perform system maintenance responsibilities. Authorised persons supervise all external personnel performing maintenance activities.

1.6 ICT Security and Policy

ICT Security and Policy Section is responsible for establishing and maintaining organisation-wide information security policies, standards, guidelines and procedures.

1.7 Information Technology Management

Information Technology Management is responsible for establishing and maintaining organisation-wide information technology functions and procedures in support of the Postal Corporation of Kenya requirements.

1.8 Information Users

Information users are individuals who have been granted explicit authorisation to access, modify, delete, and/or utilise information by the relevant Data Owner. Users must use the information only for the purposes specifically approved by the Owner. Users must also comply with all security measures defined by the Owner, implemented by the Custodian, and/or defined by ICT Security and Policy Section. Users must additionally refrain from disclosing information (unless it has been designated as public) in their possession without first obtaining permission from the Owner. Users must additionally report all situations where they believe an information security vulnerability or violation may exist to ICT Security and Policy Section. Local management must also provide users with sufficient time to receive periodic information security training, and users are required to attend such training on a periodic basis.

PART A - INFORMATION SECURITY POLICIES

1.0 ACCEPTABLE USAGE

Objective: The Acceptable Use Policy below defines the actions which the Postal Corporation of Kenya considers to be abusive, and thus, strictly prohibited. The examples named in this list are non-exclusive, and are provided solely for guidance. If you are unsure whether any contemplated use or action is permitted, please contact ICT Security and Policy Section.

1.1 General Conduct

The Postal Corporation of Kenya encourages its employees to use the Internet, email systems, personal computers, fax machines, voice mail systems and other electronic and telephonic communications systems to further the Postal Corporation of Kenya mandate, to provide customer service and support of the highest quality, to discover and develop new ways to use resources, and to promote staff development. These systems are to be used solely for Postal Corporation of Kenya authorised purposes and the use of these systems by the employees may be cancelled at any time. The Postal Corporation of Kenya may review, audit, monitor, intercept, access or disclose any electronic and telephonic communication at any time, with or without notice to employees. Thus, the employee should have no expectation of privacy.

Employees are prohibited from transmitting on or through any of Postal Corporation of Kenya services, any material that is, in Postal Corporation of Kenya sole discretion, unlawful, obscene, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, national or international law.

2.0 DATA ASSET CLASSIFICATION

Objective: In order to achieve and maintain appropriate protection of the Postal Corporation of Kenya assets, all assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The owner, as appropriate, may delegate the implementation of specific controls but the owner remains responsible for the proper protection of the assets.

2.1 Responsibility of Data Assets

Objective: All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The owner, as appropriate, may delegate the implementation of specific controls but the owner remains responsible for the proper protection of the assets.

2.1.1 Inventory of Data Assets

All assets should be clearly identified and an inventory of all important assets documented and maintained.

2.1.2 Ownership of Data Assets

All information and assets associated with information processing facilities should be owned by a designated part of the organization.

2.1.3 Acceptable Use of Data Assets

The systems, networks, email, telephone and Internet connectivity are provided for the Postal Corporation of Kenya's use. All the Postal Corporation of Kenya's staff shall be required to comply with the *Acceptable Usage Policy*. All use of the Postal Corporation of Kenya information systems, networks, email, telephone and all other messaging systems are subject to monitoring by Postal Corporation of Kenya management to confirm compliance with the Policies and Standards stated herein.

2.2 Information Classification

Objective: To ensure that information receives an appropriate level of protection, Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. The *Information Classification Standards* should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

2.2.1 Classification Guidelines

Information is an important asset to the Postal Corporation of Kenya. Accurate, timely, relevant, and properly protected information is absolutely essential to the Postal Corporation of Kenya. To ensure that information is properly handled, all accesses to, uses of and processing of the Postal Corporation of Kenya's information must be consistent with the ISO 27001 and ICTA Standards.

2.2.2 Information Labelling and Handling

Employees in the possession of any information containing the Postal Corporation of Kenya information classification sensitivity label must maintain, propagate and if need be, re-establish this same label whenever the information changes form, format or handling technology.

2.2.3 Data Retention

Data should only be retained for the length of time that is required for the organisation, legal and/or regulatory purposes. Once the retention time has elapsed, data should be disposed of securely by the Postal Corporation of Kenya approved methods.

3.0 ACCESS CONTROL

3.1 Organisational Requirements for Access Control

Objective: To control access to information, information processing facilities and the organisations processes should be controlled on the basis of the organisations and security requirements. Access control rules should take account of policies for information dissemination and authorisation.

3.1.1 Access Control Policy

Each computer and communication system user-ID must uniquely identify only one user. Shared or group user-IDs are not to be used except with management approval and where accountability can be maintained.

The computer and communications system privileges of all users, systems, and programs must be restricted based on the need-to-know when accessing information that is confidential, based on sensitivity and criticality. Access must default to a "deny all" state only allowing access to specifically granted users, systems or programs.

3.1.2 User Access Management

Objective: Procedures are in place that cover all stages of the life-cycle of user access; i.e., from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

New user-ID provisioning request is submitted by Compliance Department and will be processed accordingly. Terminations are initiated by HR and will be processed by ICT Department within the same business day.

4.0 REMOTE ACCESS

Objective: To retain the privilege of doing off-site work, all telecommuters must structure their remote working environment so that it is in compliance with the Postal Corporation of Kenya regulations.

4.1.1 Telecommuting

Work at home (telecommuting) arrangements require senior management approval. Permission to telecommute is the decision of the involved employee's manager. Before a telecommuting arrangement can begin, this manager must be satisfied that an alternative worksite (such as a home office) is appropriate for the Postal Corporation of Kenya's work performed by the involved employee.

4.1.2 Permissible Equipment

Employees working with the Postal Corporation of Kenya at alternative worksites must use Postal Corporation of Kenya provided computer or network equipment. An exception will be made only if other equipment has been approved as compatible with the Postal Corporation of Kenya's information systems and controls.

4.1.3 Storage of Sensitive Data

At no time during the use of remote access is any confidential or internal data allowed to be stored or printed on any remote media from the Postal Corporation of Kenya's secure network.

4.1.4 Remote Authentication

All remote access to the network by employees, administrators, and third parties to the Postal Corporation of Kenya's environment require multi-factor authentication for all connectivity.

5.0 PASSWORD

Objective: All users must follow the password policies listed below for all systems and implement passwords according to the standards set forth by ICT Security and Policy Section.

5.1.1 User Responsibilities

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users.

5.1.2 End User Passwords

All user-chosen passwords for computers and networks should be difficult to guess. Passwords must be complex, meaning that they must have both numeric and alphabetic mixed-case characters and at the minimum 8 characters in length. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456abcd" should not be employed. Personal details such as spouse's name, license plate, personal identification number, and birthday should not be used unless accompanied by additional unrelated characters. All user passwords will be set to expire to ensure periodic change.

5.1.3 Password Re-use and Lockout

Users must not construct passwords which are identical or substantially similar to passwords that they had previously employed the previous five (5) times.User accounts will be locked out after multiple failed login attempts.

5.1.4 Suspected Compromise

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

5.1.5 Keeping Passwords Confidential

Passwords must not be written down and left in a place where unauthorized persons might discover them.

5.1.6 Prohibition of Password Sharing

Personal user-IDs and passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to liability for actions that the other party takes with the password. If users need to share computer resident data, they should use public directories on local area network servers or other approved mechanisms.

5.1.7 Group ID Conditions

In computer centre control areas, service provider environments and specific end-user environments, user IDs or passwords can give access to functions that need to be used by a group of people. If the functionality/usability of the software does not allow for individual accountability to be maintained, user-IDs or passwords may be shared by the group under the following conditions:

- Use of the user ID or password is managed through administrative control.
- Access is only for those functions to which the group is approved.
- All members of the group are authorized to the data for which the user ID has access.

6.0 INCIDENT MANAGEMENT

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of the Postal Corporation of Kenya's assets. All users of the Postal Corporation of Kenya systems are required to report any information security events and weaknesses as quickly as possible to the ICT Security and Policy Section department or through the ICT Helpdesk.

6.1.1 Reporting Information Security Events and Weaknesses

All employees, temporary employees and third party users of information systems and services are required to note and report any observed or suspected security issues or weaknesses in systems or services.

6.1.2 Reporting Information Security Events

Information security events must be reported through appropriate management channels as quickly as possible. Events may include, but should not be limited to: loss of service, equipment or facilities, system malfunctions or overloads, human errors, uncontrolled system changes, malfunctions of software and hardware and access violations.

All contractual arrangements made with the Postal Corporation of Kenya third party service providers must require the vendor to take appropriate actions to address incidents of unauthorized access to the Postal Corporation of Kenya's information, including notification to ICT Security and Policy Section as soon as possible of any such incident, to enable the Postal Corporation of Kenya to expeditiously implement its response program.

6.1.3 User Responsibility Discovering Weaknesses

Employees, temporary employees and third-party contractors should not attempt to prove suspected security weaknesses. Testing weaknesses, with the exception of management approved Vulnerability Management program, might be interpreted as a potential misuse of the system and could also cause damage to the information system or services.

6.1.4 Contact with Authorities

Appropriate contacts with relevant authorities should be maintained. The Asst. General Manager of ICT (AGM), through guidance of ICT Security and Policy Section and the legal office, shall determine when and who may contact the authorities. Both parties will analyse the legal requirements of the incident to determine the parties that will be contacted.

7.0 PHYSICAL SECURITY

Objective: Physical security requirements should be implemented commensurate with the identified risks. Procedures should be implemented to prevent unauthorized physical access, damage, and interference to the Postal Corporation of Kenya's premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. Access rights to secure areas must be regularly reviewed, updated, and revoked when necessary.

7.1.1 Physical Security Perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities. All areas with sensitive information will be further secured with additional security controls to prevent unauthorized access. Video surveillance equipment will be used to monitor all sensitive areas and have a minimum of three (3) months of footage stored.

7.1.2 Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

All persons conducting work at the Postal Corporation of Kenya locations are required to visibly wear a badge. Contractors shall be escorted when working in sensitive areas or with confidential data. All visitors are required to visibly wear a "Visitor" badge and be escorted if dealing with vital and sensitive information or areas.

7.1.3 Securing Offices, Rooms and Facilities

Physical security for offices, rooms, and facilities should be applied. When working with confidential data both electronically and in physical form, it should be secured at all times to protect the information.

7.1.4 Clear Desk / Clear Screen

Sensitive or critical organisation information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

Computers and terminals should be logged off or protected with a screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism when unattended.

8.0 WORK STATION SECURITY

Objective: Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use and storage facilities secured to avoid unauthorized access.

8.1.1 Security of Equipment Off-premises

Security shall be applied to off-site equipment taking into account the different risks of working outside the Postal Corporation of Kenya premises. Equipment and media taken off the premises should not be

left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when traveling.

8.1.2 Remote Office Controls

Remote office controls should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office.

9.0 ANTI-VIRUS

Objective: To protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, trojan horses, and logic bombs.

9.1.1 Anti-virus Software

Anti-virus software shall be enabled on Microsoft Windows and the other appropriate system or systems which are used to access the Postal Corporation of Kenya's networks. The software must detect, remove and protect against viruses and other forms of malicious software, including spyware and adware. Tampering with or disabling anti-virus software is prohibited.

9.1.2 Unauthorized Software

Users should not install any software without consulting with ICT Security and Policy. Only Postal Corporation of Kenya approved software should be purchased or downloaded from a reputable source.

10.0 WIRELESS

Objective: To ensure that all Postal Corporation of Kenya networked systems have the controls needed to prevent unauthorized access.

10.1.1 Multi-Use Networking Equipment

Users must not establish electronic bulletin boards, local area networks, wireless access points, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of ICT Security and Policy Section.

10.1.2 Mobile Devices

When not in use, mobile devices should have their wireless capabilities disabled.

11.0 PRIVACY

Objective: To ensure confidential and Postal Corporation of Kenya private data is not disclosed in an unauthorized manner.

11.1.1 Expectation of Privacy

The work stations, laptops, and user accounts given to the Postal Corporation of Kenya'susers are to enable them to perform their jobs in the most efficient and effective way possible. However, users should not have an expectation of privacy in the materials that are created, sent, or received by them on the Postal Corporation of Kenya'ssystems. To the extent permitted by the laws and regulations, the Postal Corporation of Kenya's authorised personnel may examine all material stored on the Postal Corporation of Kenya's systems without prior notice (some examples of situations may include investigation for a suspected breach of security, or for the prevention or detection of crime, and other legally permissible situations).

11.1.2 Monitoring of Computer Usage

Subject to the laws and regulations, the Postal Corporation of Kenya may monitor any and all aspects of its computerised resources, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet, and reviewing email sent and received by the Postal Corporation of Kenya users.

Wherever possible, monitoring will be carried out by methods which prevent misuse. Users understand that the Postal Corporation of Kenya may use automated monitoring software to monitor material created, stored, sent or received on the Postal Corporation of Kenya's network to ensure that inappropriate material is not created on, or transmitted via the Postal Corporation of Kenya systems, and that inappropriate use of the Postal Corporation of Kenya's systems does not occur.

11.1.3 Right to Examine Systems

All information sent over the Postal Corporation of Kenya's computer and communications systems are the property of the Postal Corporation of Kenya. To properly maintain and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. As the Postal Corporation of Kenya computer and communication systems must be used for the organisation's purposes only, workers should have no expectation of privacy associated with the information they store in or send through these systems.

12.0 BUSINESS CONTINUITY

Objective: To counteract interruptions to the Postal Corporation of Kenya activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. In order to avert potential interruptions to business activities, to protect critical business processes from the effects of major failures of information systems or disasters, to ensure timely

resumption, and to minimize damages, the Postal Corporation of Kenya shall develop *Business Contingency Plans* (BCP) for each of its facilities and for each major application or general support system.

12.1.1 Employee Responsibilities

Employees are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts the Postal Corporation of Kenya's activity. All personnel shall be trained on contingency and recovery procedures. The plan recovery capabilities and personnel shall be tested annually to identify weaknesses.

12.1.2 Scope and Resources

To ensure the Postal Corporation of Kenya protective efforts are prioritized, efficient and effective, Senior Management will identify and designate those processes and supporting information resources which have a high organizational impact based on financial considerations, mission criticality, content sensitivity, regulatory, fiduciary or contract mandates. ICT Security and Policy, in conjunction with Senior Management, is responsible for developing a written *Business Impact Analysis*.

The procedures for execution of the business continuity plan shall be documented in writing by ICT Security and Policy Section and shall be reviewed annually, updated as necessary, and presented to the Board for approval. The plan will assign specific responsibilities to designated staff to facilitate the recovery and/or continuity of critical and essential functions. The *Business Continuity Plan* will be distributed to the Board, Executive Management, key personnel, and a copy must be stored off-site.

Resources necessary to ensure viability of the procedures shall be acquired and maintained. ICT Security and Policy Section is responsible for verification and coordination of prompt correction of all deficiencies. The plan shall be updated accordingly and status reports will be made to the Board on at least an annual basis.

12.2.1 Backup Requirements

All information stored on backup media will be encrypted to further secure the confidential and sensitive data stored. All backup media will be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility.

Back-up information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

In situations where confidentiality is of importance, back-ups must be protected by means of encryption. All data is required to be encrypted on all removable media at all times. All back-up media is required to be classified so all confidential data can be accounted for.

All media that is stored at a secondary location will be logged when it is removed and returned to the primary location at both the primary site and the storage location. During transit, all media will physically be secured to protect assets from theft and damage. A review of all media will be conducted and all media confirmed to be in the correct location.

13.0 THIRD PARTY SECURITY

Objective: To maintain the security of the Postal Corporation of Kenya's information and information processing facilities that are access, processed, communicated to, or managed by external parties.

13.1.1 Third Party Risk Assessments

Where there is a business need for working with external parties that may require access to the Postal Corporation of Kenya's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

13.1.2 Third Party Non-Disclosure Agreements

Prior to sending any secret, confidential, or private information to a third party for copying, printing, formatting, or other handling, the third party must sign the Postal Corporation of Kenya'snon-disclosure agreement. If data is shared with any third party, then the third party must sign an agreement stating they must adhere to the requirements and that they are responsible for the data that they are storing and securing.

13.1.3 Third Party Connections

Access by external parties to Postal Corporation of Kenya's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party.

13.1.4 Access Control

This document contains specific procedures covering: permitted access methods, the authorisation process for user access and privileges, and a process for revoking access rights of authorised individuals.

14.0 SECURITY AWARENESS

Objective: All employees of the Postal Corporation of Kenya and, where relevant, contractors and third party users will receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

14.1.1 Personnel Ethics

All employees are required to adhere to the *Employee Code of Conduct* and the *Employee Code of Ethics*, which provides a framework for guiding the conduct of the Postal Corporation of Kenya's employees and applying ethical standards in their work.

14.1.2 Acceptable Use

The Postal Corporation of Kenya's information and resources must be used in an approved, ethical and lawful manner. All users must abide by the Postal Corporation of Kenya's policies on acceptable use of information resources and by the *Acceptable Use Standards*. Confidential information should only be transmitted over the Internet when protected in accordance with the *Information Classification Standards*.

All users must promptly report suspicious activities or actual occurrence of any unauthorized activities, which includes unauthorized use of accounts, logon IDs, passwords, PINs, or tokens.

Employees should always be alert to actions and activities they may perform that could breach the prohibited activities outlined in the *Acceptable Use Standards*. In case employees have any doubt or queries on the appropriateness of their actions, they should clarify their understanding with their supervisor and/or ICT Security and Policy Section before performing the activities.

All the Postal Corporation of Kenya's employees must attend a yearly Information Security Training Program. This program will go over basic information security principle as well as Postal Corporation of Kenya specific information security standards.

15.0 HUMAN RESOURCES

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities, and liabilities and are equipped to support organisational security policy in the course of their normal work and to reduce the risk of human error.

15.1.1 Terms and Conditions of Employment

As part of their employment, employees, contractors and third party users shall agree and sign the Postal Corporation of Kenya *Employee Code of Conduct* and the *Employee Code of Ethics*, which states their own and the organization's responsibilities for information security.

15.1.2 Background Checks

Due to the sensitivity of the data that the Postal Corporation of Kenya handles, background checks are conducted on all employees who will have access to sensitive data or the sensitive data environment. This includes employees working with data or critical systems. Examples of background checks include pre-employment, criminal and reference checks.

PART B - INFORMATION TECHNOLOGY SECURITY POLICIES

1.0 SERVER SECURITY

Objective: All assets must be properly identified and classified accordingly. Server class machines require both physical and logical security. Servers and appliances should be kept and protected in a limited access environment with proper environmental protection. Access to servers should be limited to job functionality and given on a least privileged access philosophy.

1.1.1 Baseline Configuration

All Postal Corporation of Kenya systems, whether connected to the Internet or not, should be properly hardened. The Postal Corporation of Kenya will not operate platforms for which the vendor no longer provides security updates and patches. Security updates and patches will be tested and applied to all applicable systems in a timely manner.

Every machine on the Postal Corporation of Kenya network will have an identified owner who will be responsible for providing the requisite security for that machine.

1.1.2 Back-ups

Back-up copies of information and software should be taken and tested regularly.

The extent and frequency of back-ups should reflect the requirements of the Postal Corporation of Kenya, the security requirements of the information involved, and the criticality of the information to the continued operation of the Postal Corporation of Kenya.

The back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

In situations where confidentiality is of importance, back-ups must be protected by means of encryption. All customer data is required to be encrypted on all removable media at all times. All back-up media is required to be classified so all confidential data can be accounted for.

All media that is stored at a secondary location will be logged when it is removed and returned to the primary location at both the primary site and the storage location. During transit, all media will

physically be secured to protect assets from theft and damage. A quarterly review of all media will be conducted and all media confirmed to be in the correct location.

1.1.3 Access Control

Access control to servers shall meet the requirements set forth by the asset owner and its business and regulatory requirements. Access to the system is based on the premise that "Everything is generally denied unless expressly permitted" rather than "Everything is generally permitted unless expressly denied".

User registration and de-registration procedures should be in place for granting and revoking access to all information systems and services. Registration process should also include checking that the level of access granted is appropriate to the business purpose and is consistent with the information security policy and does not compromise segregation of duties.

1.1.4 Protection Against Malicious Code

Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

To promptly detect and prevent the spread of computer viruses, all the Postal Corporation of Kenya servers should run integrity checking software/activity nonrioting software. This software detects changes in configuration files, system software files, application software files, and other system resources. Integrity checking software should be continuously enabled or run daily.

Virus checking programs approved by ICT Security and Policy Section must be continuously enabled on all local area network (LAN) servers and networked personal computers (PCs). Installed anti-virus programs should be capable of detecting, removing, and protecting against multiple forms of malicious software, including spyware and adware.

2.0 WORK STATION SECURITY

Objective: To prevent loss, damage, theft or compromise of assets and interruptions to the Postal Corporation of Kenya activities. Equipment should be protected from physical and environmental threats. Protection of equipment is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also include equipment sitting and disposal.

2.1.1 Equipment Sitting and Protection

Workstations handling sensitive information should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use, and storage facilities secured to avoid unauthorized access.

2.1.2 Equipment Maintenance

Workstations should be maintained in accordance with the supplier's recommended service intervals and specifications. Only authorised staff should carry out repairs and service equipment.

2.1.3 Secure Disposal or Re-use of Equipment

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

3.0 CHANGE MANAGEMENT

Objective: Inadequate control of changes to the information processing facilities and systems is a common cause of system or security failures. Unauthorised changes to test, development and production systems could result in a compromise to the Postal Corporation of Kenya's network. Operational systems and application software should be subject to strict change management control.

3.1.1 Change Management Required for Operational Systems

Changes to information processing facilities and systems shall be subject to strict change management control. Change requests must be thoroughly planned, tested and approved by all relevant persons.

3.1.2 Business Requirements

Changes to operational systems should only be made when there is a valid reason to do so, such as an increase in the risk to the system. Updating systems with the latest versions of operating system or application is not always in the organisations interest as this could introduce more vulnerabilities and instability than the current version.

4.0 APPLICATION DEVELOPMENT SECURITY

Objective: To ensure that security is an integral part of information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

4.1.1 Security Requirements Analysis and Specification

Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. Specifications for the requirements for controls should consider the automated controls to be incorporated in the information system, and the need for supporting manual controls.

4.1.2 Internally Developed Applications

All software developed by in-house staff, and intended to process sensitive, valuable, or critical information, must have a written specification. This specification must be part of an agreement between the involved information owner(s) and the system developer(s).

4.1.3 Input Data Validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

4.1.4 Output Data Validation

Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate.

4.1.5 Operational Software

The updating of the operations software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization.

Operational systems should only hold approved executable code, and not development code or compilers.

4.1.6 Protection of System Test Data

Test data should be selected carefully, and protected and controlled. The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided.

When using operational data for testing purposes, the access control procedures, which apply to operational application systems, should also apply to test application systems.

5.0 MONITORING

Objective: Systems should be monitored and information security events should be recorded. Logs and fault logging should be used to ensure information system problems are identified.

An organisation should comply with all relevant legal requirements applicable to its monitoring and logging activities.

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

5.1.1 Audit Log Generation

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of and compliance with security measures.

5.1.2 Fault Logging

Faults should be logged, analysed and the appropriate actions taken. It should be ensured that error logging is enabled, if this system function is available.

5.1.3 Security Related Information

Computer systems handling sensitive, valuable, or critical information must securely log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.

5.1.4 Clock Synchronization

All multi-user computers connected to the Postal Corporation of Kenya's internal network must always have the current time accurately reflected in the internal clock.

5.1.5 Administrator and Operating Logs

System administrator and system operator activities must be logged. All user-ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user-IDs must be securely logged.

6.0 NETWORK SECURITY

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure. The secure management of networks, which may span organisational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.

7.1.1 Network Controls

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

7.1.2 Security of Network Services

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

7.1.3 Use of Network Services

Users should only be provided with access to the services that they have been specifically authorised to use. Network access should be based on a least privileged access and should be granted only to users with approved access requests.

7.1.4 Information Exchange Policies and Procedures

Formal exchange policies, procedures and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

7.1.5 Exchange Agreements

Exchanges of software and/or data between the Postal Corporation of Kenya and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. This policy does not cover release of information designated as public (marketing materials, help wanted postings, etc.).

Agreements should also include the following security conditions:

- Management responsibilities for controlling and notifying transmission, dispatch and receipt
- Procedures for notifying sender of transmission, dispatch, and receipt
- Establish incident notification contacts for security related incidents
- Responsibilities and liabilities in the event of information security incidents, such as loss of data
- Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected
- Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations

7.1.6 Third Party Confidential Information

Unless specified otherwise by contract, all confidential or proprietary information that has been entrusted to the Postal Corporation of Kenya by a third party must be protected as though it is the Postal Corporation of Kenya's confidential information.

8.0 VULNERABILITY MANAGEMENT

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities. Technical vulnerability management should be implemented in an effective, systematic and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

8.1.1 Control of Technical Vulnerabilities

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

8.1.2 Vulnerability Remediation

Based on the results of a formal risk assessment, vulnerabilities will be addressed according to the business value and level of risk. Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following the information security incident response procedures.

8.1.3 Patching

Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated or will be more harmful to the systems. If no patch is available, other controls should be considered, such as turning off services or capabilities related to the vulnerability, adding access controls to network borders or firewalls, and increasing monitoring to detect or prevent actual attacks.

8.1.4 Prohibition Against Testing Information System Controls

Users must not test, or attempt to compromise internal controls unless specifically approved in advance and in writing by ICT Security and Policy Section.

8.1.5 Prohibition Against Exploiting Systems Security Vulnerabilities

Users must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been

granted. All such vulnerabilities and deficiencies should be promptly reported to ICT Security and Policy Section.