



DRAFT SECURITY GUIDELINES FOR THE POSTAL AND COURIER SECTOR IN KENYA

DRAFT

1. INTRODUCTION

The Communications Authority of Kenya (CA) is mandated under section 47 (c) of the Kenya Information and Communications Act, 1998 to promote development of postal systems and services in accordance with recognized international standards, practices and public demand.

Subject to Section 12 of the Kenya Information and Communications (postal and courier regulations) Regulations, 2010; a licensee is required take reasonable steps to improve mail security and combat postal crimes that include among others.

2. BACKGROUND

The security of mail remains an unaddressed security gap for players in the postal/courier sector. With increased demand and adoption of postal/courier services and last-mile delivery it is critical that the service providers take precautions in how they handle mail and packages.

These guidelines are aimed at boosting consumer confidence in the postal/courier sector by implementing mechanisms that provide for, among others, enhanced security for packages, tracking of packages and compliance with set delivery standards

3. CITATION

These guidelines may be cited as Security Guidelines for the Postal and Courier sector in Kenya.

4. EFFECTIVE DATE OF THE GUIDELINES

These guidelines shall come into effect once executed and published by the Authority

5. SCOPE

These guidelines serve to provide the minimum physical and process security requirements applicable to critical facilities and handling of mail by the postal and courier licensees as licensed under Kenya Information and Communications Act, 1998 (hereafter referred to as; the “Act”).

5.1 Objectives of the guidelines and Standards

The guidelines are intended to:

- a) Improve the general security of mail and courier items;
- b) Minimize the exposure of mail and courier items to the risk of loss, theft, damage and/or interference; and

- c) Maintain and improve Licensees performance in the handling of mail and courier items for the good of the whole postal sector.

5.2 Terms and definitions

The following definitions shall be applicable for these guidelines, unless the context requires otherwise:

“Access control” refers to the practice of restricting entrance to a property, a building, or a room to authorized individuals;

“Agent” person / entity involved in any part of the provision of postal services in respect of a mail item

“Courier services” means any specialized service for the collection, dispatch, conveyance, handling and delivery of postal articles;

"data" means information recorded in a format in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium;

“Damage” – means any physical injury to a mail item (other than that caused by interference or accidental damage) occurring after the time of acceptance of that mail item by the relevant Licensee and before its delivery to the person to whom or at the premises to which it is addressed;

“Delivery” – means postal process in which a postal item leaves the responsibility of the licensee by being handed over to, or left for collection by, the addressee, or an authorized representative, or deposited in a private letter-box accessible to one or other of these;

Employees - means persons that have been engaged on a permanent, temporary, casual or part-time basis or workers (including those engaged under contract to provide services), who are (or may be) involved in conveying, receiving, collecting, sorting, delivering or otherwise handling or have access to mail items in the course of their work;

Interference - means tampering with a mail item contrary to relevant laws and regulations;

Licensee - means the holder of a postal and courier license;

Loss - means the physical unavailability of a mail item for delivery to the consignee due to any reason other than:

- (i) having been stolen,
- (ii) being incorrectly addressed,

at any time after the acceptance of that mail item by the Licensee and before its delivery to the person to whom or at the premises to which it is addressed, within 15 working days of its due day of delivery;

“Parcel” means a postal article which is posted at the office of a licensee as a parcel or is received at another office;

“Post office” means any building, house, room, receptacle, vessel, vehicle or place where postal articles are received, delivered, sorted, made up or dispatched;

“Postal article” means any article or thing transmissible by post, including but not limited to letters, aerogrammes, postcards and parcels but does include such article or thing as the Commission determines not to be transmissible by post;

“Serious incident” means a harmful event that occurs on a site during operations;

“Screening” means examination of mail by technical or other non-intrusive means that is intended to identify and/or detect explosives

6 Guidelines

6.1 Information regarding physical security measures of the outlet

- 6.1.1 Physical security requirements for critical postal facilities shall include, as appropriate a combination of security measures such as;
- a) Perimeter barriers,
 - b) Adequate lighting,
 - c) Locking mechanisms and key control,
 - d) Uniformed or identifiable security guards/personnel,
 - e) Closed-Circuit Television (CCTV) and alarm/intrusion detection system

6.2 Security of Mail

- 6.2.1 Licensees must establish, maintain and adhere to policies and procedures in relation to the security of premises, vehicles and equipment in the collection, conveyance or delivery of mail items.
- 6.2.2 Licensees shall verify the contents of any item for postage in order to determine its qualification of acceptance, conveyance or delivery.
- 6.2.3 Licensees shall establish a mail handling area which must be separate from postal /outlet Service space and provided adequate security measures.
- 6.2.4 Licensees shall ensure that there is controlled access to its mail center and handling areas by its employees or contractors with mail handling responsibilities.
- 6.2.5 Licensees should ensure that **ALL** mail areas are visible to supervisors.
- 6.2.6 Licensees must allocate responsibility to specific personnel within their organizations for the implementation of and compliance with the policies and procedures specified in paragraph 6.1.
- 6.2.7 The policies and procedures should include:
- a) Regular risk assessment;
 - b) The maintenance of records so that Licensees can identify, as far as is reasonably practicable, which Employees were responsible for the conveyance, receipt, collection, sortation, delivery or handling of specific mail items that have been interfered with; and
 - c) The measures to be taken, including monitoring, to prevent or detect loss or theft of, damage to, or interference with, mail items from or at premises, vehicles or equipment.
- 6.2.8 Licensees must reasonably regularly review the policies and procedures and, where necessary, update or amend those policies and procedures to ensure that they continue to meet the Mail Integrity Objectives.

6.3 Identifying and Handling Suspicious Items

- 6.3.1 Each licensee shall ensure that all mail and packages are screened for suspicious items once they are received in the mailroom for sorting.
- 6.3.2 Licensees shall display a list of suspicious letter and package indicators in its mailroom and provide a copy of the list to all staff to ensure they are familiar with it.
- 6.3.3 Licensees shall develop and put in place a mechanism and plan for screening suspicious items. The plan shall have the following:
 - a) A mail center security supervisor responsible for developing mail security guidelines and ensuring compliance.
 - b) Establishment of lines of communication between the mail center security supervisor, and the security office.
 - c) Screening procedures for all incoming items and package deliveries. All employees shall be trained in the procedures.
 - d) Procedures of handling of items identified as suspicious and dangerous.
 - e) Procedures for confirming the contents of suspicious letters and packages identified through screening and/or plain eyesight.
 - f) Training of all employees on mail security guidelines
- 6.3.4 If a licensee identifies a suspicious package they should subject to the procedures as stipulated by code of practice on integrity of mail.

6.4 Information and Reporting Requirements

- 6.4.1 A licensee shall ensure that all incidents of loss or theft of, damage to, or interference with mail items must be recorded in reasonable detail, which will include:
 - a) The date, time and place of the incident;
 - b) The number of (or estimate) mail items involved in the incident;
 - c) The Employees involved in the conveyance, receipt, collection, sortation, delivery or handling of the mail items involved in the incident; and
 - d) Any other particulars relating to the incident which it would be reasonable to record.

6.4.2 Incidents which are ranked as "Serious Incidents" are to be reported to Authority as soon as reasonably practicable and, in any event, within 48 hours of the Licensee becoming aware of their occurrence.

6.4.3 All Licensee must submit on quarterly basis a report detailing all incidents that have taken place, which will include:

- a) The number of mail items which were lost, stolen, damaged or interfered with during the period; and
- b) Actions taken for each of the incidents.

6.5 Employee's security

6.5.1 General

Postal and courier employees play an important role in operations and as such its fundamental to the licensees to ensure that any potential security risks as a result of new employees, existing employees and parties are mitigated.

6.5.2 Recruitment of Employees

6.5.2.1 A Licensee shall:

- a) Establish, maintain and adhere to a recruitment policy designed to facilitate the achievement of the Mail Integrity Objectives; and
- b) Allocate responsibility to specific personnel within its organization for the implementation of and compliance with that recruitment policy.

6.5.2.2 The recruitment policy shall include:

- a) An explanation of the jobs, roles or types of work, as the case may be, in respect of which the recruitment policy should apply;
- b) The types of information about a prospective Employee that the Licensee requires;
- c) The steps to be taken to satisfy itself of the identity of the prospective Employee;
- d) The steps to be taken to confirm a prospective Employee's work history over at least the immediately preceding five (5) years;
- e) A requirement for prospective Employees to declare any criminal convictions, cautions or conditional discharges for offences relating to:

- (i) Postal Packets; or
- (ii) Dishonest conduct generally (in particular, theft, obtaining property by deception or fraud)

f) Guidelines on how any such issues will be taken into consideration.

6.5.2.3 Licensees shall put in place mechanism to monitor implementation of, and compliance with, the recruitment policy.

6.5.2.4 Licensees must review, update and amend the recruitment policy on a regular basis to ensure that it continues to meet the Mail Integrity Objectives.

6.6 Training of Employees

6.6.1 Personnel security and training shall be deployed in order to reduce and minimize security risks to the business, its customers and employees.

6.6.2 If a Licensee employs or uses employees, the Licensee shall:

- a) Establish, maintain and adhere to a training policy that provides for Employees to receive initial and ongoing training so as to facilitate achievement of the Mail Integrity Objectives; and
- b) Allocate responsibility to specific personnel within its organization for the implementation of and compliance with that policy.

6.6.3 All Employees must be made aware of the seriousness of the offences related to postal offences detailed in relevant laws and regulations. The training should address the following concerns:

- a) Basic postal/courier security procedures.
- b) Safe Mail handling procedures
- c) Recognition and reporting of suspicious letters or packages.
- d) Proper use of personal-protection equipment.
- e) Response protocols for a chemical, biological, radiological, or bomb threat

6.6.4 The training policy shall include:

- a) The levels of training required to facilitate achievement of the Mail Integrity Objectives, according to the needs of different roles;
- b) A clear outline of how the training will be provided;
- c) The frequency with which training should be provided; and
- d) Details of how training will be documented and monitored.

6.7 Licensees must reasonably regularly monitor implementation of and compliance with the training policy.

6.8 Disciplinary Procedures

6.8.1 If a Licensee employs or uses employees, the Licensee shall:

- a) Ensure that employees are aware of the standards of conduct required to facilitate achievement of the Mail Integrity Objectives; and
- b) Establish, maintain and adhere to a disciplinary policy in relation to the treatment of Employees who fail to meet the standards of conduct expected of them.

6.8.2 The standards of conduct and disciplinary policy should be such as to facilitate achievement of the Mail Integrity Objectives.

6.8.3 Licensees shall allocate responsibility to specific personnel within their organizations for:

- a) Making Employees aware of the standards of conduct expected of them; and
- b) The implementation of and compliance with the disciplinary policy.
- c) A process to identify consistent failure to meet the relevant standards of conduct and the taking of appropriate remedial action.

6.8.4 Licensees shall regularly monitor implementation of and compliance with the:

- a) Standards of conduct; and
- b) Disciplinary policy.

6.9 Service Delivery Contractor security requirements

6.9.1 Under such circumstances such Licensee shall ensure that, so far as is reasonably practicable, all:

- a) Its franchisees, agents or sub-contractors involved in the conveyance, receipt, collection, sortation, delivery or handling of Postal articles, comply with this Guidelines and Standards for applied to the franchisee, agent or sub-contractor; and
- b) Its agents or sub-contractors (if any) who are responsible for providing employees to work for the Licensee, comply with these guidelines and standards applied to such agent or sub-contractor.

6.10 Review of the Guidelines

- 6.11 These guidelines will form the code of conduct for mail security operations in postal courier service provision. The same may be reviewed from time to time, to ensure that it meets the Authority's statutory obligations in as far as its approach towards securing Postal and Courier subsector.

DRAFT