1 Introduction

The Communications Authority of Kenya (hereinafter referred to as the Authority) is established under the Kenya Information and Communications Act, 1998 to license and regulate Postal, Information and Communications services in Kenya.

The Authority's objectives and mandate are spelt out in the Kenya Information and Communications Act, 1998 and ICT Sector Policy Guidelines.

The objectives include *inter alia*:

a) To contribute to overall Government objectives towards human, social and economic development through facilitating universal access and use of ICTs.
b) Further the advancement of technology relating to the ICT sector;
c) Promote development of ICT systems and services in accordance with recognized international standards, practices and public demands;
d) Foster growth, competition and investment in the sector;
e) Protect the rights of users of ICT services;
f) Ensure the development and formulation of adequate standards for the ICT sector in the country; and
g) Ensure operators' compliance with the Act, Regulations and Licensing Conditions;

Some of the specific tasks undertaken by the Authority in relation to its mandate include:

a) Licensing and regulating all systems and services in the ICT sector, including radio-communications, telecommunications, postal/courier services, broadcasting, multimedia, electronic commerce and transactions services;
b) Facilitating the development of electronic commerce (E-Commerce) and transactions;
c) Protecting consumer rights within the ICT environment ;
d) Managing competition in the sector to ensure a level playing ground for all players;
e) Monitoring the activities of licensees to enforce compliance with the license terms and conditions as well as the law.

2 Promotion of E-Commerce

In considering the promotion of E-Commerce and other online transactions, the Authority takes note of the important role of the Internet and its potential in enhancing such businesses as logistics and supply chain management. This provides immense opportunities for postal and courier operators.

A typical E-commerce environment is illustrated in the figure below:

E-COMMERCE AND SUPPLY CHAIN MANAGEMENT

It is however noted that the uptake of E-Commerce is still low despite the high growth in various ICT related services in the country.. It is with this in mind that the Authority has developed these guidelines whose objective is to facilitate the uptake of E-Commerce in the country.

These guidelines are aimed at boosting consumer confidence in e-commerce by requiring Postal/Courier operators to implement mechanisms that provide for, among others, remote payment options, enhanced security for packages, tracking of packages and compliance with set delivery standards.

3 Specific Guidelines

The following are guidelines intended to specifically promote E-Commerce:

I. Remote Payment Guidelines

All Postal/Courier licensees are required to put in place procedures by which customers can pay for services remotely. These procedures entail incorporating a secure remote payment platform through a licensed financial payment services provider. Licensees are at liberty to implement a payment option that accords them the greatest flexibility in their operations.

II. Security Guidelines

All operators are required to ensure their operations conform to the security standards set out in the Postal Security Guidelines. These are outlined in Annex 1(A&B).

III. Delivery Standards.

These guidelines relate to maximum expected timelines to be met by licensees when delivering parcels on a non-expedited basis. The parcel delivery geographical area is defined as, a County, a County Headquarter or an Urban Centre within a county. The delivery timelines are defined in terms of days.

These standards therefore dictate the maximum timelines to be met while transporting parcels within a County or between Counties. Licensees may choose to offer expedited parcel delivery which shall exceed the minimum set delivery standards for ordinary/non-expedited delivery. The ordinary/non-expedited delivery standards are set out in Annex 2.

IV. Guidelines on Tracking of Postal Items

These guidelines relate to the measures licensees should put in place to enable their customers ascertain the status of their packages prior to delivery. The objective is to enable customers ascertain the location of packages and expected time of delivery.

a. Inbound and Outbound International Packages

This relates to all packages transported into or out of the country. International Courier Operators are required to put in place electronic automated mechanisms by which a customer can track their package to ascertain its location. . The automated mechanism should be able to:

i. Indicate the time and location a package was received by the courier.

ii. The current estimated location.

iii. The expected delivery location and estimated delivery time.

Automated mechanisms may take the form of, but not limited to:

- Proprietary web-based tracking systems
- Email-based tracking systems/updates.
- SMS-based tracking systems/updates.
- IVR-based tracking systems.

b. Local Packages

This relates to all packages transported within the country. National Courier Operators are required to put in place either automated or non-automated mechanisms by which a customer can track their package to ascertain its location. The automated mechanism should be able to:

i. Indicate the time and location a package was received by the courier.

ii. The current estimated location.

iii. The expected delivery location and estimated delivery time.

For non-automated mechanisms, a National Courier operator may choose to either:

- Set up a Call Centre or
- Provide a Customer Care telephone number for tracking enquiries.

National Courier operators may choose to incorporate automated tracking mechanisms.

Annex 1

A: Postal/Courier Security Management Framework

	Proposed Standards/Measures	Rationale	Responsibility
1)	Mail shall not be left unattended or in an insecure environment at any time and must be kept in secured receptacles, under guard, CCTV or other monitoring	Unsecured mail has been the cause of mail loss, pilferage and theft.	All Operators
2)	All staff shall be trained in security /training with a security champion. The training areas should include: • Basic postal security and investigations • Emergency planning and risk assessment • Airport security coordination and quality of service/security reviews • Countering of drug trafficking and money laundering through the post • Procedures for accepting and controlling the induction of dangerous goods • Identification of prohibited goods • Revenue accounting and protection	Lack of requisite training has been the cause of inefficiency and admittance of illegal and prohibited items into the postal/courier network	All Operators
3)	High-risk mail comprising of insured and valuable items e.g. lab samples, specimens, medicines etc. shall be afforded appropriate protection through such measures as insurance, tracking etc	Safety of critical items in the network requires additional guarantees.	All Operators

4)	Systems shall be taken to prevent unauthorised persons from accessing operational sites. Such systems should include provision of staff photo IDs, name cards and security passes.	Security threats are real in the country and should be forestalled.	All Operators
5)	Deployment of effective supervisory checks to safeguard mail. This shall be done through declaration of contents and obtaining identification details of senders at points of acceptance among other measures.	There have been many cases of operators accepting for transmission offensive and scurrilous materials whose senders cannot be traced.	All Operators
6)	Equipment used to deliver mail shall be given adequate security at all times through such measures as satellite-tracking of mail vehicles and lockable receptacles for mail, among others.	Cases of attack on mail vehicles and theft of mail in transit have been reported	All Operators
7)	An annual risk assessment shall be conducted to identify each critical facility. The assessment shall take into consideration the postal/courier assets and operations at the facility, the general crime rate of the area and other contributing factors that increase the likelihood of criminal incidents. For each critical facility, a detailed written security plan shall be developed and maintained. The security plan shall contain the following control measures: - facility design standards; -perimeter barriers; -perimeter windows, doors or other openings;	Risk assessment and critical facility security plans	Designated Operator

	-lighting; -locking mechanisms and key controls;		
8)	All critical facilities shall be constructed to conform to national design standards for safety and security and contain resilient materials to preclude illegal entry. A designated program of annual inspection and repair shall be conducted to assure the integrity of structures including timescales for completion of any repair. The annual inspection shall also include a risk assessment of the immediate vicinity, the profile of the mail product being processed and any other changes in the operation that may affect the security of the building and its employees.	Critical facility design standards	Designated Operator
9)	Physical barriers such as fencing, walls, and vehicle gates shall be installed to deny access of un-authorized individuals or vehicles to restricted areas of the critical facility. Perimeter fences or dividing walls shall be set back from the critical facility (to increase the likelihood of observing intruders attempting to breach the secure area). The areas adjacent to the perimeter fencing shall be kept free of debris, trees and shrubbery (so they cannot be used to violate the secure area). Weekly inspections of the perimeter barriers shall be conducted to ensure their integrity.	Perimeter barriers	Designated Operator
10)	An adequate access control process shall be put in place for secure (non-customer) areas of all critical postal facilities. A manual access control system shall be implemented: i. uniformed security guards, a receptionist or other personnel staff shall be at entry/ exit points to verify the entry privileges for each individual; ii. the manual process shall be documented in a standard operating procedure;	Access control systems for employees, visitors, service providers and vendors to ensure admittance of authorized personnel only.	All Operators

	iii. training and instructions shall be provided to the respective personnel administering the system and the individuals stationed at the fixed access control point; iv. a registration system shall be maintained to record entries of non-employees into secure areas of the critical facility. In addition, an automated (electronic) or hybrid access control system shall be implemented in areas deemed to be of high risk. The system shall be designed to prohibit unauthorized entries of individuals through the entry/exit points and only through a single access system or process and shall be a single access system to only permit entry for the respective badge holder which activates the access point. A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.		
11)	Only official vehicles or approved contract vehicles shall be permitted in areas used to load/transport mail or other secure exterior operations areas. Entrance to these areas shall be clearly marked and placarded to ensure awareness of the boundaries of the restricted area. A manual or automated access control system shall be used to ensure unauthorized vehicles do not gain access into the secure exterior operations area. If it is necessary for a non-official vehicle to enter the secure exterior operations area, a procedure shall be in place to verify the identity of the driver and if necessary to inspect the vehicle before entering the secured area. Employee parking areas shall be assigned a location separate from the vehicle operations areas. Visitor parking shall be separate from secure vehicle operations areas.	Access control systems for vehicles to premises to ensure no illegal entry.	Designated Operator
12)	A personnel and visitor identification system shall be implemented to allow for positive	Identification systems	All operators

	identification of employees and visitors when entering the critical facility. Postal personnel (career, temporary or contract employees) shall be provided with easily identifiable identification badges featuring their legal name as documented in the Human Resource system, their unit/department, role, photograph and expiration date. The Postal Security Unit or other postal managers shall be responsible for the control, issuance and removal of employee, visitor and contractor identification badges. A process shall be maintained to report and communicate employee information. An authorized permit system shall be used to identify all vehicles while operating in any secure exterior operations areas. The permit shall be current and visibly displayed.	enhanced to control entry by unauthorized persons	
13)	The personnel selection and hiring policy shall be documented for all employees working within the facilities of the DO or handling mail at external locations. The hiring policy shall be consistent with national legislation to ensure prospective and current employees and contractors qualified to perform postal duties as a person of integrity. Background screening (criminal history or police checks) for all career employees shall be conducted consistent with national legislation. A process shall be maintained to report and communicate employee performance and misconduct. The hiring process shall include interviews, pre-employment data verification and other screening measures commensurate with positions or duties. The termination process shall be documented for employees and contractors to ensure the timely return of identification documents, access control devices, keys, uniforms and other sensitive information. A record system shall be maintained to prevent re-hiring of terminated employees or contractors.	Personnel security and hiring processes : to ensure integrity of staff handling mail	Designated Operator
14)	Security awareness training programs shall be documented and maintained for all	Awareness and training	All operators

	employees and contractors. Where appropriate, the postal/courier operator offering international mail service shall implement a dangerous goods training program commensurate with International Civil Aviation Organization (ICAO) and the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air or National Authority. The training shall be delivered to acceptance personnel, individuals who interface with the customers for mail induction and individuals handling mail articles at the office of exchange. The content of the training course shall provide individuals with an awareness of dangerous goods regulations, prohibited items and the acceptance of permissible dangerous goods as prescribed by the Universal Postal Union (UPU) or the Authority. The awareness training shall include the following: i. General description of dangerous goods; ii. United Nations hazard classes and labeling; iii. Types of products which may contain dangerous goods; iv. Acceptance verification and handling procedures; v. Permissible categories of dangerous goods for transport by air; vi. Packing instructions and labeling requirements for permissible dangerous goods to be transported by air.	measures :there is limited awareness and training among the postal/courier staff	
15)	The postal/courier operator shall tender items to carriers, ground handling agents or other contractors for transport on aircraft in identifiable bags or containers affixed with the appropriate forms or receptacle labels. All receptacles/consignments shall be accompanied by the appropriate documentation or its electronic equivalent as applicable	Measures for mail accepted/inducted for carriage on commercial aircraft	All operators

	After screening or the application of other security controls, mail shall be accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier, ground handling agent or other contractor. The postal/courier operator or respective border agency/customs authority/security authority shall conduct a risk assessment consistent with national standards, legislation and international aviation security guidance to determine if specific mail items pose an elevated risk. Elevated risk items shall be subjected to additional security controls consistent with the requirements of the National Civil Aviation Security Program.		
16)	The postal/courier operator and authorized contractors shall document processes and procedures for security of the mail by all modes (air, road, sea and rail) of transportation. The postal/courier operator shall comply with all applicable national legislation regarding transportation standards. Access to mail shall be restricted as appropriate to postal employees or contractors with mail handling responsibilities. Mail transport vehicles shall be designed from resilient materials and possess features such as a solid-top, hard sides or reinforced soft-sides and locked cargo doors. When vehicles loaded with mail are in transit or left unattended outside of secure postal or contractor premises the vehicle and all access points to the mail shall be secured (locked). Vehicles or conveyances shall be clearly marked or be indicated as denoting that it is an authorized postal vehicle or postal contracted vehicle. Transport operators (postal or contractor) shall wear a designated postal uniform and/or possess and clearly display a valid form of postal or contractor identification. Vehicle cabin and ignition keys for all transport vehicles shall be secured from unauthorized access.	Transportation and conveyance security requirements for DO's and postal contractors	All operators

	A key accountability process shall be maintained. Routes, schedules and planned stops shall be assessed for risk and, if necessary, an additional security measure shall be initiated to mitigate the risk. Vehicles, conveyance or containers shall be properly emptied.		
17)	An annual risk assessment shall be conducted to identify each critical facility. The assessment shall take into consideration the postal assets and operations at the facility, the general crime rate of the area and other contributing factors that increase the likelihood of criminal incidents. For each critical facility, a detailed written security plan shall be developed and maintained. The security plan shall contain the following control measures: - facility design standards; -perimeter barriers; -perimeter windows, doors or other openings; -lighting; -locking mechanisms and key controls;	Risk assessment and critical facility security plans	Designated Operator
18)	The postal/courier operator shall have a documented security program covering the areas of prevention and investigation for the protection of mail, employees, partners, customers and postal assets. This shall be communicated to all employees. The postal/courier operator shall have a dedicated Postal Security Unit or dedicated personnel to perform safety and security measures. The staff members dedicated to these functions shall be commensurate with the size and operations of the postal/courier operator. The dedicated Postal Security Unit or dedicated security personnel shall perform periodic	Postal security unit for prevention and investigative management (minimum security requirement)	All operators

	facility and process security reviews.		
19)	The postal/courier operator shall document and communicate to all employees a documented: -crisis plan to ensure the security of mail, employees, customers and postal assets in the event of a man made or natural disaster that would affect the flow of mail or postal operations; -business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations; -Hazardous material response plan and/or team for spillage procedures and/or handling dangerous goods. Hazardous material incidents shall be documented and reported to the appropriate authorities in a timely manner.	Disaster recovery, emergency preparedness and business continuity planning	All operators
20)	When dispatching mail consisting of all international letter post items up to 500 grams, as defined in Letter Post Regulations, the DO may dispatch it without additional screening if the DO has adhered to the security measures outlined in UPU Standard S58. UPU member countries may agree to permit exemptions from screening or the use of alternative security measures because of the special nature of some types of mail. Such exemptions should be clearly defined in UPU member countries' National Civil Aviation Security Program, and may include the following: o high-value items; o diplomatic mail, in accordance with the provisions of the Vienna Convention;	Items exempt from screening	Designated Operator

	○ live animals such as livestock or pets. Accompanying materials such as feedbags, cages and containers should be subjected to security controls; ○ vaccines and other perishable medical items; ○ life-sustaining items such as blood, blood products, bone marrow and human organs intended for transplant originating from authorized entities; ○ human remains and the necessary packaging; and ○ special nuclear materials. The above categories may be exempted from screening provided they are: ○ clearly declared on shipping documents as such; ○ physically checked on receipt for any signs of tampering; ○ subject to documentary checks and direct verification, such as by a telephone call to the consignor, in order to establish their bona fides; and • – continually protected against unauthorized interference.		
21)	Consignments of an international operator shall be screened using the most appropriate method to the type of consignment. *NOTE 1 A screening method may be inefficient and ineffective when it is not suited to the type of consignment being inspected. In some cases, a single screening method may not be sufficient to inspect all types of mail therefore, more than one method should be readily available. DOs should apply an appropriate and effective screening method for each consignment and ensure that all personnel carrying out the screening are properly trained and supervised. Screening equipment should be maintained, tested and operated in accordance with the manufacturer's instructions.* Mail items comprise of the following mail classes: Express, Letter Post (literature for the	Items to be screened	All operators

	blind, small packets, printed paper, letter-post items), and Parcels. The DO or designee shall screen items by at least one of the following methods in accordance with the requirements of their National Civil Aviation Security Programme (NCASP). As a minimum, the NCASP should reflect the Standards and Recommended Practices set forth in ICAO Annex 17 and the guidance material in ICAO Aviation Security Manual, Doc 8973. o EDD; o EDS; o ETVD; o manual search; o metal detection; ▪ – X-Ray equipment or other wave based systems		
22)	Mail that requires additional security measures beyond baseline procedures, such as visual inspection or single aspect screening, to be applied to it is considered high risk. Mail or mail items can be considered high risk if there are: ▪ anomalies in its nature that give rise to suspicion such as evidence of tampering; ▪ due to its nature, baseline security measures alone are unlikely to detect dangerous goods as defined in the UPU and CA regulations; ▪ specific intelligence or threat information about it; ▪ reasons to suspect that it contains or poses a threat based on risk assessment by an appropriate authority for aviation security, aircraft operators or other actors in the supply chain. The DO or designee shall screen (EDS or X-Ray) high-risk items:	High risk items that could pose potential security risks especially terror related in the region.	

	○ by viewing the item or receptacle from two angles and complying with National legislation, OR • Utilizing a combination of two or more screening methods below: • Manual search; • X-Ray equipment; • EDD; • ETD.		
23)	When designated, the DO or designee shall utilize technologies below to screen items already contained in receptacles/bags: – X-Ray screening technology that allows the DO to view the item or receptacle from two views/angles: i. The DO shall X-ray one receptacle at a time to search for indications of unauthorized explosives, incendiaries, and other destructive substances or items. ii. Mail receptacles containing commodities that are too dense to render an accurate X-ray image shall be screened twice in succession, rotating the receptacle 90 degrees horizontally in either direction prior to screening it the second time, iii. If the X-ray image is unclear, shielded, or opaque or contains any unidentifiable anomalies, the DO shall clear the X-ray image by removing each mail piece from the receptacle and re-screen the individual pieces. and/or – EDD; and/or	Screening procedures for mail receptacles/bags	Designated Operator

	– EDS.		
24)	When designated, the DO or designee shall utilize technologies below to screen items already contained in receptacles/bags: – X-Ray screening technology that allows the DO to view the item or receptacle from two views/angles: i. the DO shall X-ray one receptacle at a time to search for indications of unauthorized explosives, incendiaries, and other destructive substances or items. ii. mail receptacles containing commodities that are too dense to render an accurate X-ray image shall be screened twice in succession, rotating the receptacle 90 degrees horizontally in either direction prior to screening it the second time, iii. if the X-ray image is unclear, shielded, or opaque or contains any unidentifiable anomalies, the DO shall clear the X-ray image by removing each mail piece from the receptacle and re-screen the individual pieces and/or – EDD; and/or – EDS.	Screening procedures for mail receptacles/bags to further enhance security	Designated Operator