



***Communications for all in East Africa***

## **EAC POSTAL SECURITY GUIDELINES**

**Prepared by EACO  
JUNE 2025**

# 1 TABLE OF CONTENTS

1.	INTERPRETATION .....	4
2.	ABSTRACT .....	6
3.	INTRODUCTION.....	7
4.	CITATION .....	7
5.	IMPLEMENTATION OF THE POSTAL AND COURIER SECURITY GUIDELINES.....	7
6.	SCOPE .....	7
7.	OBJECTIVES OF HARMONISATION OF POSTAL AND COURIER SECURITY IN EAST AFRICAN COMMUNITY (EAC) .....	8
8.	EAC POSTAL AND COURIER GUIDELINES.....	9
8.1	Critical postal and couriers' facilities security requirements and Adoption of Screening Protocol. ....	9
8.1.1.	Physical Security Requirements .....	9
8.1.2.	Adoption of Screening Protocol.....	9
8.2	Procedures for accepting and controlling the induction of dangerous goods and hazardous materials.....	10
8.3	Procedures for Implementation of robust cybersecurity measures .....	10
8.4	Access Control Systems .....	11
8.4.1	Access control systems for employees, visitors, service providers, and vendors ...	11
8.4.2	Access control Procedures for transportation of Postal Articles .....	11
8.4.3	A personnel visitor Identification systems.....	12
8.5	Security Personnel Hiring Processes .....	12
8.5.1	Contractor Security Requirements .....	13
8.5.2.	Awareness and Training Measures .....	13
8.6	Procedures for Compliance audit program and oversight.....	14
8.7	Postal /courier security unit for prevention and investigative management .....	15
8.8	Security of postal /courier articles and Safety of Persons .....	15
8.9	Information and Incident Reporting Requirements.....	16
8.10	Establishment of partnerships and information-sharing mechanisms with law enforcement agencies, regulatory authorities, and other stakeholders.....	16
8.11	The Postal articles carriers, ground handling agents, or other contractors for transport on aircraft in identifiable bags or containers affixed with the appropriate forms or receptacle labels. ....	17

<b>8.12</b>	<b>The postal/courier operator and authorized contractors document processes and procedures for the security of the postal and courier articles by all means (air, road, sea, and rail) of transportation.....</b>	<b>17</b>
<b>8.13</b>	<b>Annual risk assessment and Disaster recovery, emergency preparedness, and business continuity planning.....</b>	<b>18</b>
<b>9.</b>	<b>AMENDMENT OF THE GUIDELINES .....</b>	<b>20</b>

## 1. INTERPRETATION

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

**“Agent”** person or entity involved in any part of the provision of postal services in respect of postal articles. The agent includes both employees of and subcontractors to the postal articles service contractor, together with the employees of and subcontractors to other agents. They also include devices, equipment, and property of the aforesaid which are utilized in the provision of postal services for the item concerned;

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

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

**“Delivery and acceptance”** - A postal article shall be considered delivered and accepted if; (a) to have been delivered to the addressee (i) when it is delivered into a private letter box or bag of the addressee; (ii) when it is left at the house, or office of the addressee as set out thereon, or with the employee, agent or any other person authorized to receive it; or (iii) where the addressee is a guest or is a resident at a hotel, hostel or lodging, when it is left with the proprietor or manager of the hotel, hostel or lodging or with his agent; or (b) to have been received by a postal licensee when it is deposited into a posting box or handed over to an employee or agent of a postal service operator authorized to receive it.

**“Interference”** - means tampering with a postal article contrary to relevant laws and regulations;

**“Loss”** - means the physical loss of a postal article, other than as a result of:

- (a) having been stolen,
- (b) being incorrectly addressed,

at any time after the acceptance of that postal article 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;

**“Postal item”** means postal article

**“Parcel”** is a postal item weighting from 0 up to 30 kg that contains a good with basic attributes such as tracking, liability and signature on delivery.

**“Small packets”** is a postal item weighting from 0 up to 2 kg that contains a good with basic attributes such as tracking, liability and signature on delivery.

**“Postal article”** means material goods, with or without mercantile value, that comply with the post ability requirements determined by the Act and its regulation, and that are delivered via a physical network to a specified address or a person with a specified address;

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

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

**“Verify”** means the process of confirming the s declared by the consignor

**“Critical postal facility”** means the office of exchange; air office or unit; postal/courier facilities where aviation security screening is completed; and the final facility where postal articles transit before dispatch via air.

**“Suspicious Item”**– refers to any postal article that is highly unusual compared to those that are typically processed.

## **2. ABSTRACT**

The East African Community (EAC) trails to strengthen the security and efficiency of its postal and courier sectors through the harmonization of security guidelines. This initiative responds to the increasing complexity of security threats and the need for a cohesive approach to safeguarding postal and courier services across member states. The harmonization process involves a thorough assessment of existing security protocols within member states, identifying discrepancies and areas for improvement. The developed guidelines cover a broad range of security aspects, including risk assessment and management, parcel screening and monitoring, staff training, and emergency response procedures. By adopting these standardized measures, the EAC aims to improve the resilience of its postal and courier networks against potential threats, ensure compliance with international best practices, and foster a secure environment for the growth of regional trade and communication. Furthermore, the document provides actionable recommendations for implementing the harmonized guidelines, including mechanisms for regular review and updates to address emerging security challenges. Through this collaborative effort, the EAC will enhance the safety and reliability of its postal and courier services, ultimately contributing to regional stability and economic development. This document outlines a comprehensive framework designed to standardize security practices, address common vulnerabilities, and facilitate enhanced cooperation between EAC countries. Likewise addresses the need for harmonization of security guidelines within the East African Community (EAC) to enhance the integrity and efficiency of postal and courier operations. By establishing a unified framework, the harmonization aims to address common security threats, streamline operational protocols, and facilitate cross-border cooperation.

### **3. INTRODUCTION**

Postal and Courier Security is paramount in facilitating safe services within the East African region by upholding principles of confidentiality, integrity, fraud prevention, counterterrorism, cross-border trade facilitation, public health, and cybersecurity. Postal and Courier authorities can foster trust, promote economic development, and enhance regional connectivity through the postal and courier network. East Africa member States shall collaborate in joint programmes to improve and secure postal and courier items to assault crime, adopt programmes and actions to promote security, prioritise the functions of operational control and inspection ; investigation through the adoption of an appropriate organic and functional structure, the assignment of the necessary human and functional resources ; and the formulation of regulations which facilitate interaction between the security of postal sector ;the external national and international agencies.

### **4. CITATION**

These guidelines may be cited as Security Guidelines for the Postal and Courier operators in the East African Community (EAC).

### **5. IMPLEMENTATION OF THE POSTAL AND COURIER SECURITY GUIDELINES**

Implementation of Harmonization postal and courier security guidelines in EAC requires a comprehensive approach involving stakeholder engagement, careful planning, and continuous evaluation. By aligning security practices, organizations can enhance their ability to handle security threats effectively, improve operational efficiency, and build greater trust with customers.

### **6. SCOPE**

These Guidelines shall apply to all postal and courier operators in East Africa region, their franchisees, agents, or sub-contractors involved in the conveyance, receipt, collection, sortation, delivery, or handling of postal articles.

## **7. OBJECTIVES OF HARMONISATION OF POSTAL AND COURIER SECURITY IN EAST AFRICAN COMMUNITY (EAC)**

EAC Member States shall collaborate in joint programmes to: -

- a) adopt regulations and enact laws to protect the post and courier against crime and establish specific agencies for the enforcement of such laws;
- b) render technical assistance for the development and establishment of operational control and inspection services; and for the technical training of personnel of the postal and courier administrations;
- c) ensure the consultation of the inspection and postal security services in the design of postal and courier buildings, installations and operating systems involving postal and courier items;
- d) regularly conduct surveys, studies and investigations about materials and equipment which make the items more secure;
- e) establish a permanent regional network for security and inspection services to promote the exchange of technical and administrative information and joint actions;
- f) encourage the protection of postal and courier committed to airlines, regulate procedures for receiving from and delivering postal and courier dispatches to airlines and computerizing documentation;
- g) encourage joint development and adoption of security measures by surface or maritime carriers;
- h) encourage automation or mechanization of systems;
- i) Combat illegal drug traffic;
- j) disseminate information on security and crime to carrier of postal and courier items and employees;
- k) collect statistics to identify weaknesses; and
- l) Intensify actions to ensure postal and courier items are safe from dangerous and hazardous materials in line with international practices.

## **8. EAC POSTAL AND COURIER GUIDELINES**

Guidelines for security of postal and courier are crucial for ensuring the safe and efficient handling items and packages. Here are security guidelines typically for postal services and organizations responsible for postal and courier items handling within the East African Community (EAC).

### **8.1 Critical postal and couriers' facilities security requirements and Adoption of Screening Protocol.**

#### **8.1.1. Physical Security Requirements**

Physical security requirements for critical postal and courier facilities are essential and should consider the following: -

- (a) Perimeter fencing and barriers;
- (b) Gets and entry points with electronic access control systems;
- (c) Closed-circuit television (CCTV), alarm systems, and monitoring stations;
- (d) Uniformed or identifiable on-site - security guards;
- (e) External and internal lighting;
- (f) Radio Communications systems;
- (g) Security audit and maintenance check; and
- (h) Ensure that environmental controls, such as climate control and fire suppression systems, are in place to protect physical assets.

#### **8.1.2. Adoption of Screening Protocol**

Effective screening helps identify security threats such as explosives, weapons, or hazardous materials, mitigating risks to postal articles and should include:

- (a) Manual inspection
- (b) X-ray equipment or other wave-based systems
- (c) Standard Operating Procedures (SOPs)
- (d) Provision of comprehensive security training for postal and courier employees in security /training with security champions.

## **8.2 Procedures for accepting and controlling the induction of dangerous goods and hazardous materials**

Procedures for accepting and controlling the induction of dangerous goods and hazardous materials should include: -

- (a) Identification and classification of prohibited goods upon receipt;
- (b) Train staff for better equipped to identify and respond to security threats, contributing to the overall resilience of the postal system;
- (c) Verify all documentation provided by the sender, including shipping papers, labels, and safety data sheets, before accepting the goods;
- (d) Conduct a thorough inspection of the packaging and labeling to ensure compliance with regulations and to check for any signs of damage or leakage and Implement criteria for accepting dangerous goods, including verification of the goods.
- (e) Ensure all dangerous goods are documented and labeled according to regulatory requirements, including hazard symbols, handling instructions, and emergency contact information.
- (f) Maintain comprehensive documentation for each batch or shipment of dangerous goods, including details of the goods, their classification, and the handling procedures used.

## **8.3 Procedures for Implementation of robust cybersecurity measures**

Procedures for the implementation of robust cybersecurity measures should include the following: -

- (a) encryption, and user authentication mechanisms, to protect postal systems and data;
- (b) Network Security by deploying firewalls, Intrusion Detection and Prevention Systems (IDPS); and Segmentation of networks;
- (c) Develop comprehensive cybersecurity policies that define acceptable use, data protection, incident response, and other critical security practices; Establish procedures for implementing and enforcing policies, including incident response protocols and regular security assessments, and provide ongoing cybersecurity

training and awareness programs to educate employees about security best practices, phishing, and social engineering threats.

- (d) Develop and maintain an incident response plan that outlines procedures for detecting, responding to, and recovering from cyber incidents, form an incident response team with clearly defined roles and responsibilities to manage and respond to security incidents and conduct post-incident reviews to analyze the cause of the incident, assess the response, and improve security measures.

## **8.4 Access Control Systems**

### **8.4.1 Access control systems for employees, visitors, service providers, and vendors**

An adequate access control process shall be in place for secure (non-customer) areas of all critical postal and courier operators' facilities. It may consist of one or a combination of the following:

- (a) Manual access control system;
- (b) Uniformed security guards, a receptionist, or other personnel staff shall be at entry/egress points to verify the entry privileges for each individual, the manual process shall be documented in a standard operating procedure;
- (c) Training and instructions shall be provided to the respective personnel administering the system and the individuals stationed at the fixed access control point; and
- (d) A registration system shall be maintained to record entries of non-employees into secure areas of the critical facility and access control system.

### **8.4.2 Access control Procedures for transportation of Postal Articles**

Postal and Courier Operators should use the following access control procedures for the transportation of postal articles: -

- (a) Only official or approved contracted means of transport shall be permitted in areas used to load/transport postal articles or other secure exterior operations areas;
- (b) Entrance to these areas shall be marked and placard to ensure awareness of the boundaries of the restricted area;

- (c) A manual or automated access control system shall be used to ensure unauthorized means of transport do not gain access to the secure exterior operations area;
- (d) If a non-official or third-party means of transport must 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;
- (e) Employee parking restricted areas shall be assigned a location separate from the operations areas; and
- (f) Visitor parking shall be separate from secure operations area

#### **8.4.3 A personnel visitor Identification systems**

- (a) A personnel and visitor identification system shall be implemented to allow for the identification of employees and visitors when entering the critical facility;
- (b) Postal / courier 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, photograph, and expiration date. Other information such as access level, and department/unit, may be added as required by local regulations and legislation;
- (c) The Postal /courier Security Unit 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; and
- (d) The permit shall be current and visibly displayed.

#### **8.5 Security Personnel Hiring Processes**

- (a) The personnel selection and hiring policy shall be documented for all employees working within the facilities of the licensee or handling postal articles at external locations;
- (b) The hiring policy shall be consistent with national legislation to ensure prospective and current employees and contractors are qualified to perform postal/courier duties as a person of integrity;

- (c) Background checks (criminal history or police checks) for all career employees shall be conducted consistent with national legislation;
- (d) A process shall be maintained to report and communicate employee performance and misconduct;
- (e) The hiring process shall include interviews, pre-employment data verification, and other confirmation measures commensurate with positions or duties;
- (f) The termination process shall be documented for employees and contractors;
- (g) The termination process shall ensure the timely return of identification documents, access control devices, keys, uniforms, and other sensitive information; and
- (h) Record shall be maintained to prevent the re-hiring of employees or contractors who have been terminated due to misconduct.

#### **8.5.1 Contractor Security Requirements**

- (a) Contractors performing postal and courier handling/transport operations or other sensitive functions shall apply personnel security measures equivalent to the licensee; and
- (b) The contractor shall inform the licensee of any illegal findings or decisions that could pose potential security risks to the operation.

#### **8.5.2. Awareness and Training Measures**

- (a) Documented security awareness training must be provided to all employees and contractors;
- (b) Security requirements must be documented for licensee and postal/courier contractors, covering all transportation modes;
- (c) Processes for securing postal articles during transportation (by air, road, sea, or rail) must be documented, and compliance with national transportation standards is required;
- (d) Access to postal articles should be restricted to authorized personnel with postal articles handling responsibilities;
- (e) Postal/ courier means of transport should be built with resilient materials and features like solid tops, hard sides, or reinforced soft sides, and must have secure cargo doors. Vehicles should be inspected for tampering before loading;

- (f) Postal articles mean of transport must be secured (locked) when in transit or left unattended outside secure premises;
- (g) Means of transport should be clearly marked as postal and courier or contractor vehicles when possible;
- (h) Transport operators should wear postal or courier uniforms or display valid postal or contractor identification;
- (i) Means of transport cabin and ignition keys must be secured from unauthorized access.
- (j) A key accountability process must be maintained;
- (k) Routes, schedules, and stops should be assessed for risks, with additional security measures implemented if needed;
- (l) Means of transport and containers must be properly emptied; and
- (m) Postal articles mean of transport must be secured (locked) when in transit or left unattended.

#### **8.6 Procedures for Compliance audit program and oversight**

- (a) An annual compliance audit shall be conducted by personnel independent of the critical facility management team.
- (b) The individuals conducting the compliance audit review shall be afforded the necessary authority to obtain relevant information and to enforce corrective action.
- (c) The compliance audit review program covers the entire postal article security program to ensure the implementation of security requirements. The compliance audit review program shall include, but not be limited to, an emphasized focus on facility security, personnel security, and transportation and conveyance security.
- (d) The licensee shall ensure that the management of the compliance audit review program is independent of individuals responsible for the implementation of security requirements.
- (e) Records of the compliance audits and recommendations shall be maintained.
- (f) The result of the compliance audits shall be reported to the executive management of the licensee. Follow-up actions shall be monitored and documented.

## **8.7 Postal /courier security unit for prevention and investigative management**

- (a) The licensee shall have a documented security program covering the areas of prevention and investigation for the protection of postal articles, employees, partners, customers and postal assets. This shall be communicated to all employees.
- (b) The licensee shall have a dedicated Postal and Courier Security Unit or dedicated personnel to perform safety and security measures.
- (c) The staff members dedicated to the security functions shall be commensurate with the size and operations of the licensee.
- (d) The dedicated Postal Security Unit or dedicated security personnel shall perform periodic facility and process security reviews.

## **8.8 Security of postal /courier articles and Safety of Persons**

Licensees shall establish and implement policies and procedures to provide for the safety of persons and security of premises, vehicles, and equipment involved in the collection, conveyance, or delivery of postal articles. The requirement on the safety of persons also applies to any third party in the vicinity of postal articles, but not directly involved in the collection, conveyance, or delivery of postal articles;

- (a) The policies and procedures shall provide for the process of identification and handling of prohibited articles and suspicious postal articles;
- (b) The policies and procedures should incorporate risk assessment and shall at a minimum provide for;
- (c) Allocation of responsibilities to specific personnel within the organizations for the implementation of and compliance with the policies and procedures;
- (d) Establishment of a postal articles handling area which must be separate from the postal/outlet service area;
- (e) Controlled access to the postal articles centre and handling areas by its agents with postal articles handling responsibilities.
- (f) The process of verifying the contents of postal articles to determine their qualification of acceptance, conveyance, or delivery.

- (g) The mechanism and plan for the screening and dealing with prohibited articles and suspicious postal articles;
- (h) The measures to be taken to prevent, detect, and address the loss, theft, damage, or interference with postal articles; and
- (i) Licensees shall ensure the policies and procedures are regularly reviewed.

### **8.9 Information and Incident Reporting Requirements**

- Licensees shall ensure that all incidents of loss, theft of, damage to, or interference with postal articles, are recorded in reasonable detail, which shall include:
  - (a) The date, time, and place of the incident;
  - (b) The number of (or estimate) postal articles items involved in the incident; and
  - (c) Any other particulars relating to the incident which it would be reasonable to record such as the value of the item.
- Licensees shall submit every quarter a report detailing all incidents that have taken place, which shall include: The number of postal articles items that were lost, stolen, damaged, or interfered with during the period; and actions taken for each of the incidents.
- Incidents that are ranked as "Serious Incidents" shall be reported to the Authority as soon as reasonably practicable and, in any event, within 48 hours of the licensee becoming aware of their occurrence.

### **8.10 Establishment of partnerships and information-sharing mechanisms with law enforcement agencies, regulatory authorities, and other stakeholders**

The licensee should establish partnerships and information-sharing mechanisms with law enforcement agencies, regulatory authorities, and other stakeholders to combat postal and courier-related crimes and enhance the ability to prevent, detect, and respond to criminal activities involving postal and courier networks.

**8.11 The Postal articles carriers, ground handling agents, or other contractors for transport on aircraft in identifiable bags or containers affixed with the appropriate forms or receptacle labels.**

The licensee should abide by the following: -

- (a) All receptacles/consignments shall be accompanied by the appropriate documentation or its electronic equivalent as applicable Measures for postal articles accepted/inducted for carriage on commercial aircraft.
- (b) postal articles shall be accounted for and protected from unauthorized interference before loading on an aircraft or secure exchange with the carrier, ground handling agent, or other contractor.
- (c) 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 postal articles 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.

**8.12 The postal/courier operator and authorized contractors document processes and procedures for the security of the postal and courier articles by all means (air, road, sea, and rail) of transportation.**

- (a) The postal/courier operator shall comply with all applicable national legislation regarding transportation standards;
- (b) Access to postal articles shall be restricted as appropriate to postal employees or contractors with postal articles handling responsibilities;
- (c) Postal/courier articles 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.
- (d) When vehicles loaded with postal articles are in transit or left unattended outside of secure licensee or contractor premises the vehicle and all access points to the postal articles shall be secured (locked).

- (e) Vehicles or conveyances shall be marked or be indicated as denoting that it is an authorized postal vehicle or postal contracted vehicle.
- (f) Transport operators (postal or contractor) shall wear a designated postal operator uniform and/or possess and display a valid form of postal or contractor identification.
- (g) Vehicle cabin and ignition keys for all transport vehicles shall be secured from unauthorized access.
- (h) Transportation and conveyance security requirements for postal and courier operators and contractors
- (i) 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, conveyances, or containers shall be properly emptied.

### **8.13 Annual risk assessment and Disaster recovery, emergency preparedness, and business continuity planning**

An annual risk assessment shall be conducted to identify each critical facility. The assessment shall take into consideration the licensee assets and operations at the facility, the general crime rate of the area, and other contributing factors that increase the likelihood of criminal incidents. The assessment shall include the following: -

- (a) 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.
- (b) The postal and courier operator shall document and communicate to all employees a documented: crisis plan to ensure the security of postal articles, employees, customers, and postal assets in the event of a man-made or natural disaster that would affect the flow of postal articles or postal operations; business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations; and Hazardous material response plan and/or team for spillage procedures and/or handling dangerous goods.
- (c) Hazardous material incidents shall be documented and reported to the appropriate authorities promptly.

- (d) a business continuity plan to minimize interruption in the event of a significant incident that might impact domestic or international postal and courier operations.

**8.14 Establishing security guidelines for the process of conveyance, receipt, collection, sortation, and delivery of postal and courier articles is essential for maintaining the integrity and safety of postal articles services.**

The following are key considerations and practices that should be part of a comprehensive security guideline for handling postal articles:-

- (a) Designate areas where postal articles are processed as restricted zones. Only authorized personnel should have access and require staff to wear identification badges and implement sign-in/sign-out procedures;
- (b) Conduct regular training sessions for personnel on security protocols, recognizing suspicious behavior, and emergency response procedures and promote a security culture among employees to encourage vigilance and reporting of any unusual activities;
- (c) Ensure that drop-off points for postal articles are monitored and Implement procedures for verifying the legitimacy of items being collected, including checking sender identification and tracking numbers;
- (d) Install security cameras in sorting areas to monitor activities and deter theft or tampering and Enforce a two-person rule whenever possible during the handling and sorting of high-value or sensitive items;
- (e) Utilize secure transport vehicles with locking mechanisms and alarms for moving postal articles and Implement GPS tracking systems on vehicles transporting high-value or sensitive mail items;
- (f) Establish processes for verifying the identity of recipients upon delivery, such as requiring a signature or identification and Train delivery personnel to recognize and report suspicious packages, and establish protocols for handling them safe;
- (g) Create clear channels for staff to report security breaches, incidents, or suspicious activities and develop procedures for investigating security incidents and documenting findings for future reference;

- (h) Ensure that all facilities are equipped with secure locking mechanisms and alarm systems and Utilize physical barriers (e.g., fences, security gates) to prevent unauthorized access to facilities;
- (i) Implement policies for protecting sensitive customer information, including encryption and secure communications and Control access to digital systems and data related to postal article tracking and management;
- (j) Conduct regular security audits to assess compliance with established guidelines and identify areas for improvement and perform risk assessments periodically to evaluate potential vulnerabilities and update security measures accordingly.

## **9. AMENDMENT OF THE GUIDELINES**

This Guideline may be amended from time to time, to ensure that it meets the EAC's statutory obligations.