



BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY

POSTAL SECURITY GUIDELINES FOR BOTSWANA

MARCH 2026

Table of Contents

DEFINITIONS AND INTERPRETATION 1

PREAMBLE 3

1. INTRODUCTION 4

2. BACKGROUND 4

3. CITATION 4

4. SCOPE AND OBJECTIVES OF THE GUIDELINES 4

 4.1 Scope 4

 4.2 Objectives of the Guidelines 4

5. POSTAL SECURITY PRINCIPLES 5

 5.2.3 Adequate lighting 5

 5.2.4 Access Control 6

 5.2.5 Closed-Circuit Television and Alarm or Intrusion Detection System 6

 5.3 Physical Security 6

 5.4 Mail Processing Facilities 7

 5.4.1 Centralisation of Mail Operations 7

 5.4.2 Physical Layout of Mail Processing Facilities 8

 5.5 Vehicle Security Measures 8

 5.6 Dedicated Uniformed or identifiable Security Guards or Personnel 8

 5.6.2 Personnel Security Controls 9

 5.6.3 Compliance Awareness and Security Training 9

 5.7 Information and Incident Reporting Requirement 9

 5.8 Cybersecurity 9

 5.9 Disaster Recovery and Business Continuity Management 10

 5.10 Data Protection 10

 5.11 REVIEW OF THE GUIDELINES 10

 5.12 COMMENCEMENT 10

DEFINITIONS AND INTERPRETATION

In the event of conflict or ambiguity between the terms defined herein and the terms defined in the Licence or in the Communications Regulatory Authority Act, 2012 (CRA Act or the Act) or the Communications Regulatory Authority Regulations, the following order of precedence shall apply:

- a) The Act;
- b) The Communications Regulatory Authority Regulations;
- c) The Licence; and
- d) The Postal Security Guidelines.

In these Guidelines, any word or expression to which a meaning has been assigned in the CRA Act, shall have the same meaning, unless the context otherwise indicates:

Access Control

Physical security refers to the practice of restricting access to a property, building, or room to authorised individuals.

Note: Physical access control can be achieved by a human (a guard or receptionist), through mechanical means such as locks and keys, or through technological means such as a card access system.

Critical Facility

An office of exchange, air mail unit, or other facilities operated by postal or courier service providers to consolidate, transit, and screen postal items before conveyance.

Courier Service

Postal service with value-added delivery of addressed postal items directly to the addressee, either in terms of speed or extra services.

Damage

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.

Employees

Persons who have been engaged on a permanent, temporary, casual, or part-time basis or workers, 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

Tampering with a mail item contrary to relevant laws and regulations.

Licensee

The holder of a valid postal licence under the Communications Regulatory Act, 2012.

Postal Item

Any physical mail item conveyed through a postal network

Screening

Examination of mail using technical or other non-intrusive methods to identify and/or detect explosives and/or prohibited or restricted items.

Serious Incident

A harmful event that occurs on a site during operations.

PREAMBLE

The Botswana postal sector is undergoing a transformation due to the rise of e-commerce and online transactions. As the postal systems evolve, security concerns like mail theft, loss, damage, and misuse have also increased. To address these concerns, a well-defined legislative framework is necessary to improve mail handling security, ensure consumer protection, and maintain public trust.

Botswana Communications Regulatory Authority (BOCRA or the Authority) recognises the importance of an efficient, reliable, and secure postal system for national development and economic growth. Postal services are essential public services that facilitate business, communication, and the delivery of goods and information. It is in this regard that the Authority has developed these Postal Security Guidelines (the Guidelines) to ensure that postal service operators align with the vision for secure and effective service delivery.

These Postal Security Guidelines establish basic security requirements and promote best practices throughout the sector. The Guidelines aim to ensure uniform, risk-based approaches that align with national interests and international security requirements as prescribed by the Universal Postal Union.

1. INTRODUCTION

- 1.1** Botswana Communications Regulatory Authority is charged with the mandate to supervise the postal services in Botswana as well as to ensure that, as far as practicable, there is provision of safe, reliable, efficient and affordable postal services throughout the country. In this context, BOCRA has developed Postal Security Guidelines (the Guidelines) to promote the development of safe postal systems and services. These Guidelines adhere to internationally recognised standards, practices, and public demand, and require Licensees to take reasonable steps to enhance mail security and combat postal crimes.

2. BACKGROUND

- 2.1** With the increasing demand and adoption of postal services, security remains a challenge for postal players in the ever-changing market. It is, therefore, crucial for service providers to take precautions and enhance postal services security to build consumer confidence in the sector.

3. CITATION

- 3.1** These Guidelines may be cited as Postal Security Guidelines for Botswana.

4. SCOPE AND OBJECTIVES OF THE GUIDELINES

4.1 Scope

- 4.1.1** These Guidelines shall apply to all postal operators in Botswana involved in the provision of postal services.

4.2 Objectives of the Guidelines

- 4.2.1** The Guidelines are designed to:

- 4.2.2** Ensure the general security of postal items;

- 4.2.2.1** Minimise the risk of loss, theft, damage, and interference to postal items;

- 4.2.2.2 Implement adequate safety measures to protect life, property, and postal items; and
- 4.2.2.3 Improve and maintain the performance of Licensees in handling postal items.

5. POSTAL SECURITY PRINCIPLES

5.1 Enhancing postal security and integrity demands the daily implementation of effective measures by all service providers and relevant market players in a coordinated and consistent manner. In this context, the fundamental building blocks for operational postal security and integrity encompass management approaches and activities that align with international best practices, as outlined in this section.

5.2 General Physical Security Measures

5.2.1 Physical security requirements for critical postal facilities shall include, as appropriate, a combination of security measures such as perimeter barriers, lighting, locking mechanisms and key control, uniformed or identifiable security guards/personnel, Closed Circuit Television (CCTV) and alarm or intrusion detection systems.

5.2.2 Perimeter Barriers

5.2.2.1 A physical or virtual structure that marks a boundary and provides a layer of security deterring unauthorised access to property. Physical barriers, such as fencing, walls, and vehicle gates, shall be installed to prevent unauthorised individuals and vehicles from accessing restricted areas of the critical facility. Perimeter fences or dividing walls should allow for observation of intruders attempting to breach the secure area. Additionally, the areas adjacent to the perimeter fencing should be kept free of debris, trees, and shrubbery to prevent them from being used to violate the secure area. Weekly inspections of the perimeter barriers are essential to ensure their integrity.

5.2.3 Adequate lighting

5.2.3.1 Adequate lighting systems shall be installed in all pedestrian and vehicle entry and exit areas, exterior operations areas, parking

areas, and along perimeter fences or walls. The lighting level should illuminate these areas sufficiently to allow for the identification of individuals or vehicles within proximity. Additionally, lighting in areas near airports or runways should follow aviation authority requirements. Where CCTV is used, illuminating interior areas, including operational storage areas, should also be considered. Emergency lighting should be installed in critical operational areas.

5.2.4 Access Control

5.2.4.1 Access for pedestrian or vehicle entry and egress points shall be designed to prohibit access by non-authorized individuals. A control system shall be maintained for adequate accountability. The system shall register and record the issuance of access and shall be administered by the Postal Security Unit or the respective postal facility manager.

5.2.5 Closed-Circuit Television and Alarm or Intrusion Detection System

5.2.5.1 Operators shall use CCTV systems to monitor areas and record footage, while alarm systems detect intrusions and trigger alerts. CCTV provides visual evidence and deterrence, while alarms provide immediate notification of potential breaches.

5.3 Physical Security

5.3.1 Postal operators must maintain a safe work environment that always promotes security and integrity of mail, while protecting employees and assets. The following practices may be considered in this regard:

5.3.1.1 If the workplace has access control, employees must not be permitted to gain entrance by “piggy backing” their way in behind others;

5.3.1.2 Wherever possible, security guards must attend to all visitors and examine personal belongings brought into the building or office area;

- 5.3.1.3 Access to critical facilities must be restricted through locked or guarded entryways;
- 5.3.1.4 All storage rooms, boiler rooms, telephone and utility closets, and similar potential hiding places should remain locked or off-limits to visitors;
- 5.3.1.5 Use of distinct and separate ID badges for staff and visitors;
- 5.3.1.6 Visitors must, to the furthest extent possible, be accompanied by staff to and from the office or facility entrance;
- 5.3.1.7 Visitors should be required to display IDs to security personnel when they sign in; and
- 5.3.1.8 Logs must be kept on the arrival and departure times of all visitors.
- 5.3.1.9 Consideration should be given to the engagement of certified security experts to constantly evaluate the company's personnel and physical security safeguards. Such evaluations shall include, at a minimum: periodic risk assessments, audits of access control systems, inspection and maintenance of security equipment, monitoring of staff compliance with established security protocols, and the identification of vulnerabilities. All evaluation findings shall be documented and submitted to management, together with mandatory recommendations for corrective and preventive measures.

5.4 Mail Processing Facilities

5.4.1 Centralisation of Mail Operations

- 5.4.1.1 One of the best ways to minimise risk to employees and the public while reducing costs and increasing the efficiency and effectiveness of mail processing is to centralise mail handling at a separate, dedicated mail-processing centre or hub. Having a separate mail location reduces risk by limiting exposure to potentially dangerous mail to one location and fewer people. It also reduces costs by eliminating redundancies in locations,

staff, and equipment. Establishing trained staff to work at a single location also increases the efficiency of operations.

5.4.2 Physical Layout of Mail Processing Facilities

5.4.2.1 Properly designing a physical layout for mail centres is a preventive security measure. Some of the proven best practices in this regard include:

- 5.4.2.1.1 All work areas visible to supervisors;
- 5.4.2.1.2 Use of one-way glass, closed-circuit video surveillance cameras; or elevated supervisor stations;
- 5.4.2.1.3 Eliminating desk drawers and similar places of concealment;
- 5.4.2.1.4 Ensuring adequate supervision of mail centre staff, who may have access to high-value or high-risk mail;
- 5.4.2.1.5 Controlling access to mail centres and handling areas;
- 5.4.2.1.6 Use of sign-in/out sheets, card key access-control systems, and photo ID badges are all effective security procedures;
- 5.4.2.1.7 Access control at critical facilities should also be extended to all employees, including cleaners, maintenance staff, and visitors;
- 5.4.2.1.8 Enforcement of limited access to mail centres; and
- 5.4.2.1.9 Use of a counter or desk to separate the area where employees pick up mail from the rest of the mail centre.

5.5 Vehicle Security Measures

5.5.1 Installation of GPS tracking devices for real-time monitoring

5.5.2 Use hardened locking mechanisms.

5.5.3 Use of alarm systems

5.6 Dedicated Uniformed or identifiable Security Guards or Personnel

5.6.1 Postal operators shall appoint uniformed and clearly identifiable mail centre security coordinators or personnel to oversee operations, ensure that security protocols are followed, and assure accountability for all mail. Such personnel shall at all times be visibly identifiable through approved uniforms, service badges, or official identity cards issued by the service provider.

5.6.2 Personnel Security Controls

5.6.3 Postal Operators must ensure pre-employment screening, which should include checking the job candidate's criminal records and verification with former employers.

5.6.4 Compliance Awareness and Security Training

5.6.4.1 Engage all employees on compliance with the laws and regulations of the Republic of Botswana as well as the offences related to the provision of postal services; and

5.6.4.2 Train Security personnel appropriately to minimise security risks to the business, its customers, and employees.

5.7 Information and Incident Reporting Requirement

5.7.1 Licensees shall keep record of and submit a quarterly report to the Authority detailing all incidents that have occurred during the period, including:

5.7.1.1 The date, time, and location of the incident;

5.7.1.2 The number of mail items that were lost, stolen, damaged, or interfered with; and

5.7.1.3 Actions taken in relation to each incident. Incidents that are classified as "Serious Incidents" must be reported to the Authority as soon as reasonably possible, and in any case, within 48 hours of the Licensee becoming aware of their occurrence.

5.8 Cybersecurity

5.8.1 Postal and courier service providers shall develop and operationalise comprehensive cybersecurity policies that seek to protect and safeguard the organisation's IT infrastructure in accordance with the BOCRA Cybersecurity Baseline Security requirements for Services Providers.

5.8.2 In the event of a breach or attempted breach, postal operators shall notify the Authority within **8 hours** and activate their incident response and recovery procedures.

5.9 Disaster Recovery and Business Continuity Management

- 5.9.1 The Licensees shall develop and implement business continuity guidelines in accordance with the Business Continuity and Disaster Recovery Guidelines for the Communications Sector in Botswana 2019. Licensees shall document and communicate to employees,
 - 5.9.1.1 Disaster recovery plans 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; and
 - 5.9.1.2 Business continuity plans to minimise postal interruption in the event of significant incident which might impact domestic or international postal operations.

5.10 Data Protection

- 5.10.1 Postal and courier service providers must develop, implement, and maintain comprehensive data protection and privacy policies. These policies must ensure the lawful collection, processing, storage, and sharing of personal data in line with the Data Protection Act.

5.11 REVIEW OF THE GUIDELINES

- 5.11.1 These Guidelines shall be reviewed every five years or from time to time, to ensure that they remain relevant and enhance the security of the postal networks.

5.12 COMMENCEMENT

- 5.12.1 The Guidelines will commence implementation on July 1, 2026.