



nampost®

Mail & Logistic Postal Security Policy


Chief Executive Officer

3 DECEMBER 2022
Effective Date

This policy replaces all previous policies on this matter and became effective on the date approved by the Board of Directors.

DOCUMENT CONTROL

Created / Effective date	03 December 2021
Exco Recommendation	05 October 2021
Approved by the Board of Directors	03 December 2021
Document Owner	Executive: Mail & Logistics
Next review date	1 st of December 2023

RELATED DOCUMENTS

This policy shall be read with and implemented in conjunction with the following documents -

1. Fraud Risk Management policy
2. Crime Prevention Strategy
3. Recruitment and Selection policy
4. Annual Risk Assessment and Critical Facility Security plans
5. Universal Postal Union (UPU) Regulations, standards 58 and 59

CONTENTS

1. SCOPE.....	5
2. SECURITY MEASURES AND STANDARDS.....	5
2.7 Part A: General Security Measures.....	7
2.7.1 Access Control.....	7
2.7.2 Critical facility.....	7
2.7.3 Minimum Security Requirement.....	7
2.7.4 Screening.....	7
2.7.5 Single Access System.....	7
3. TERMS AND DEFINITIONS.....	8
Symbols and abbreviations.....	8
4. CRITICAL FACILITY SECURITY STANDARD.....	8
4.1 General Physical Security Measures.....	8
4.2 Risk Assessment and Critical Facility security plans.....	8
4.3 Critical Facility Design Standards (Minimum Security Requirement).....	9
4.4 Perimeter Barriers Fencing/ Walls (Minimum Security Requirement).....	9
4.5 Perimeter windows, doors, or other openings.....	9
4.6 Lighting.....	10
4.7 Locking Mechanisms and Key Controls.....	10
4.8 Uniformed Security Guards.....	11
4.9 Alarm or Intrusion Detection Systems.....	11
4.10 Video Surveillance Cameras or Closed-Circuit Television Systems (CCTV Systems).....	11
4.11 Access Control Measures.....	12
4.11.1 General Information Regarding Access Control Measures.....	12
4.11.2 Access Control Systems for Employees, Visitors, Service Providers and Vendors.....	12
4.11.3 Access Control Systems for Vehicles.....	13
4.11.4 Identification Systems.....	14
5. PERSONNEL SECURITY AND TRAINING.....	14
5.1 General.....	14
5.2 Personnel Security Checks and Hiring Processes.....	14
5.3 Contractor Security Requirements.....	15



6. TRANSPORTATION AND CONVEYANCE SECURITY REQUIREMENTS FOR POSTAL SERVICES AND POSTAL CONTRACTORS 16

7. TRANSPORTATION AND CONVEYANCE SECURITY REQUIREMENTS FOR POSTAL SERVICES AND FLEET CONTROLLERS 17

8. CUSTOMS PROCESSES 17

9. AWARENESS & TRAINING MEASURES (MINIMUM SECURITY REQUIREMENT) 18

10. POSTAL SECURITY UNIT FOR PREVENTION AND INVESTIGATIVE MANAGEMENT - OVERSIGHT 18

11. POSTAL SECURITY UNIT FOR PREVENTION AND INVESTIGATIVE MANAGEMENT 18

12. DISASTER RECOVERY, EMERGENCY PREPAREDNESS AND BUSINESS CONTINUITY PLANNING 19

13. APPROVAL 19



1. SCOPE

- 1.1 This document describes the physical and process security standards which are applicable to the entire postal services network. The document comprises the minimum requirements and identifies “best practices” within the postal sector.
- 1.2 Namibia Post Limited (NamPost) as a designated postal operator (DPO) under the licence issued to it by the Communications Regulatory Authority (CRAN) and postal supply chain parties can provide evidence of its compliance with National Civil Aviation Security Program (NCASP) and other internationally recognised security certification programs deemed to comply with the requirement of UPU Standards S58 and S59.

2. SECURITY MEASURES AND STANDARDS

- 2.1 The NamPost Security policy defined a minimum set of security measures, which can be applied to all facets of the postal services. Developing measurable standards of security for the postal operations contributes to protecting postal employees and assets as well as protecting postal items in general; and enabling customs authorities to apply risk assessment tools.
- 2.2 The physical and process security standards listed in this document are applicable to the entire postal network.
- 2.3 The standards are comprised of minimum requirements and identified “Best Practices” within the postal sector.
- 2.4 The main body of the standard is cited in Section 4, Physical and Process Security Standards for the Postal Sector.
- 2.5 Parts B through G of the series of standards contain specific standards for postal processes which include the mail induction process, sorting centres, the postal transportation network, and Airmail unit at the Hosea Kutako Airport and Delivery operations.
- 2.6 The series of standards documents are organised into the following parts:
 - 2.6.1 Part A:

Physical and Process Security Standards for the Postal Services – Part A: General Security Measures defines the physical and process security standards which are applicable to the entire postal Services network.

2.6.2 Part B:

Physical and Process Security Standards for the Postal Services – Part B: Mail induction process defines the physical and process security standards which are applicable to both staffed and non-staffed mail induction points.

2.6.3 Part C:

Physical and Process Security Standards for the Postal Services – Part C: Transportation security defines the physical and process security standards which are applicable to the surface transportation network.

2.6.4 Part D:

Physical and Process Security Standards for the Postal Services – Part D: Post Offices and Cash Handling at Post Offices defines the physical and process security standards which are applicable to retail units and other facilities handling cash or remittances.

2.6.5 Part E:

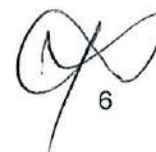
Physical and Process Security Standards for the Postal Sector – Part E: Plant/Sorting Centre security defines measures for securing operations relating to postal plants and sorting centres. The standards comprise minimum requirements and identify “Best Practices” within the postal sector.

2.6.6 Part F:

Physical and Process Security Standards for the Postal Services – Part F: Office of Exchange and airmail Security defines measures for securing operations relating to the transport of international mail.

2.6.7 Part G:

Physical and Process Security Standards for the Postal Sector – Part G: Delivery Operations defines measures for securing domestic delivery operations.



2.7 Part A: General Security Measures

2.7.1 Access Control

In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a security guard or receptionist), through mechanical means such as locks and keys, or through technological means such as a card access system.

2.7.2 Critical facility

Office of exchange, air mail unit or postal facility where aviation security screening is completed, or the final postal facility where mail items transit prior to dispatch via air. The critical facilities are also classified as the high-risk facilities for the purposes of implementing the minimum-security standards.

2.7.3 Minimum Security Requirement

This refers to the minimum-security requirements, techniques, methods, processes as well other related security measures are implemented throughout the postal operations network to secure those operations within the designated critical facilities comply to local legislation, internal policies, and procedures.

2.7.4 Screening

Examination of mail by technical or other non-intrusive means that is intended to identify and /or detect explosive as well as dangerous goods.

2.7.5 Single Access System

Physical characteristics of an Access Control System which restricts the entry of unauthorized individuals by only allowing one person to enter through the controlled area before the entry door is closed. It must prevent piggybacking or tailgating of employees without human intervention. This is usually accomplished through the use of turnstiles but may also be accomplished through a pair of doors and speciality sensors.



3. TERMS AND DEFINITIONS

Several common terms used in this document are defined in documents referred in the UPU Normative References and in the Bibliography. Definitions of frequently used or particularly important terms as well as other terms introduced in this document are given below.

For the purposes of this document, the following terms and definitions apply:

Symbols and abbreviations

- CCTV:** Closed Circuit Television System
- DPO:** Designated Postal Operator
- ICAO:** International Civil Aviation Organization
- NCASP:** National Civil Aviation Organization
- MSR:** Minimum Security Requirement
- PSG:** Postal Security Group

4. CRITICAL FACILITY SECURITY STANDARD

4.1 General Physical Security Measures

Physical Security measures for postal facilities shall include as appropriate a combination of security components such as Lighting, Locking Mechanisms and Key Control, Uniformed Security Guards, CCTV and Alarms, Panic Buttons, Fire Detection Systems, Fire Fighting systems, Perimeter Barriers, and a dedicated mail security unit.

4.2 Risk Assessment and Critical Facility security plans

4.2.1 An annual risk assessment shall be conducted to identify each critical facility. The assessment should 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's incidents.

4.2.2 For each critical facility, a detailed written security plan shall be developed and maintained. The security plan shall contain the following measure:

4.2.2.1 Critical facility design standards

4.2.2.2 Perimeter barriers

A handwritten signature or mark consisting of a stylized, cursive 'Q' or 'A' followed by the number '8'.

- 4.2.2.3 Perimeter windows, doors, or other openings:
- 4.2.2.4 Lighting
- 4.2.2.5 Locking mechanisms and key controls.
- 4.2.2.6 Access control measure.

4.3 Critical Facility Design Standards (Minimum Security Requirement)

All facilities should be constructed to national design standards for safety and security and contain resilient materials to preclude illegal entry. The integrity of the structures should be maintained through a designated program of periodic inspection and repair. The annual inspection should 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. All doors, windows and entry/egress points should be secured with the appropriate locking mechanism or visual observation by designated security personnel. Restricted areas should be well marked and secured with the appropriate access control measures.

4.4 Perimeter Barriers Fencing/ Walls (Minimum Security Requirement)

As appropriate, physical barriers such as fencing, walls, and vehicle gates should be installed to deny access of non-authorized individuals or vehicles onto restricted areas of postal facilities. Perimeter fences or dividing walls should be sufficiently separated from the facility to increase the likelihood of observing intruders attempting to breach the secure area. The areas adjacent to the perimeter fencing should be kept free of debris, trees, and shrubbery so they cannot be used to violate the secure area. Periodic inspections of the perimeter control measures must be conducted to ensure the integrity of the measure.

4.5 Perimeter windows, doors, or other openings

- 4.5.1 All exterior doors should be designed to a sufficient strength to prevent, or delay forced entry by use of portable hand tools or other means of aggression. Exterior doors and frames for non-customer areas should be fabricated of steel or a suitable alternative. The number of doors should be the minimum necessary to provide adequate access to the facility secure areas. Security signage should be placed on exterior

doors denoting restricted access and if appropriate any warnings describing responsibility and the procedures for notifying management should criminal events take place in the postal services facilities.

- 4.5.2 All exterior windows and other openings should be secured by appropriate locking mechanisms and if appropriate should be affixed with bars, mesh, or any other material to harden the access point against unauthorized entry.

4.6 Lighting

- 4.6.1 Adequate lighting systems must be installed in all pedestrian or vehicle entry/egress areas, exterior operations areas, parking areas, and along perimeter fences or walls. The lighting level must illuminate these areas sufficiently to identify individuals or vehicles within close proximity. Emergency lighting should be installed in critical operational areas.
- 4.6.2 External lighting levels should be of sufficient illumination to support high-quality CCTV images and recording. In addition, a documented periodic maintenance program should exist which ensures the operation of the lighting system and the veracity of its' use to support CCTV monitoring and recording.

4.7 Locking Mechanisms and Key Controls

- 4.7.1 All lock mechanisms for pedestrian or vehicle entry/egress points should be designed of hardened materials to prohibit access by non-authorized individuals.
- 4.7.2 A Key Control System (Register) must be established to ensure an adequate accountability of key issuance is maintained. The Key Control system should be administered by the respective Postal Security Unit. The system should register and record the issuance of keys and also protect access to non-issued keys through the maintenance of a locked key storage location.

4.8 Uniformed Security Guards

Uniformed Security Guards operating under the direction of the Postal Services are a valuable security measure to prevent and deter unauthorized entry into facilities. A written plan should be developed which identifies the risk areas to maintain an adequate security presence.

4.9 Alarm or Intrusion Detection Systems

Alarm or intrusion detection systems should be installed in high-risk facilities based upon the appropriate risk assessment. All external doors and windows in the facility will be alarmed with magnetic contacts or glass rupture detectors. Infrared or similar technology motion sensors should also be installed in appropriate areas. The system contact wires should be configured to detect device failures and a back-up configuration for alarm communication should be installed. The system should be monitored by a dedicated 24/7 control center or law enforcement authorities. System performance should be recorded for a minimum period of 60 days.

4.10 Video Surveillance Cameras or Closed-Circuit Television Systems (CCTV Systems)

4.10.1 Dedicated Video Surveillance Systems or CCTV systems should be installed to observe all external and internal areas determined to be of risk by unauthorized access or potential theft or depredation of mail or postal assets. The CCTV system should be monitored real-time and should also record/store images for a minimum period of 30 to 60 days using an analog or digital recording system.

4.10.2 The CCTV control room should be under separate security controls and should only be accessed by designated postal security personnel or postal facility managers. Camera placement locations should be selected to promote maximum coverage in the necessary areas. Color cameras (Fixed or Pan/Tilt/Zoom) provide advantages on internal configurations due to the ability of the color images to identify individuals by garment color or other personal characteristics.

4.10.3 Black and white cameras (Fixed or Pan/Tilt/Zoom) are generally more effective for identification of physical characteristics of individuals and

vehicles for exterior locations due to their higher resolution than color systems. Fixed or Pan/Tilt/Zoom (PTZ) Lenses are recommended dependent on the depth of field to be viewed.

4.11 Access Control Measures

4.11.1 General Information Regarding Access Control Measures

4.11.1.1 Access control prevents unauthorized access to post office, mail, mail conveyance vehicles, postal facilities or contract facilities which might handle, store, or process mail. It is imperative that the appropriate level of access control be implemented at every postal facility to ensure positive control of employees and visitors and protect postal assets.

4.11.1.2 Access control can be a manual process utilizing fixed security guard posts at entry/egress points to verify the identity of the individual or vehicle entering the secure area as well as conducting body search on NamPost personnel and customers if necessary. Access control measures can also consist of simple or complex electronic systems to verify and permit access to the secure areas.

4.11.1.3 Regardless of the technological aspects of the methods utilized, it is necessary that the system possess the ability to adequately screen and differentiate the access privileges of employees, visitors, service providers, and vendors at all points of entry. A properly designed access control system in a facility should be segmented to ensure that employees, visitors, service providers and vendors are only permitted access to those areas of a facility where they have work functions or conduct business.

4.11.2 Access Control Systems for Employees, Visitors, Service Providers and Vendors

4.11.2.1 An adequate access control process must be in place for the secure (non-customer) areas of all postal facilities. If a manual access control system is utilized it will be necessary to equip these entry/egress points with Uniformed Security Guards,

 12

receptionist, or other personnel to verify the entry privileges for each individual.

- 4.11.2.2 A visitor registration system must be implemented to record entries of non-employees in the secure areas of the facilities. Visitors in facilities will be escorted unless the physical design of the area in the facility they intend to access does not permit further entry into any secure operations areas. Service providers and vendors should also be escorted in postal facilities dependent on the specific circumstance of their visit.
- 4.11.2.3 A single access system can also be accomplished by assigning Uniformed Security Guard or other personnel to a fixed post to monitor the entries/egress from the access point. If the entry/egress point is not monitored, physical access control equipment (turnstiles, access gates and doors) activated by badge readers or electronic keys must be used. These systems should be designed as a single access system to only permit entry for the respective badge holder which activated the door.)
- 4.11.2.4 The access control system should consist of stand-alone distributed panels which make the access decision by referencing a central or stand-alone database. The software for the system must be capable of providing an audit trail of all who have accessed the database and all changes made by an individual. The unit must have different levels of password control to access the data or program the unit.

4.11.3 Access Control Systems for Vehicles

Only official vehicles or approved contract vehicles should be permitted in areas used to load/transport mail or other secure exterior operations areas. Entrance to these areas should be clearly marked to ensure the general public is aware of the boundaries of the restricted area. A manual or automated access control system should 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 should be in place to verify



the identity of the driver and if necessary, inspect the vehicle before entering the secured area. Employee parking areas should be assigned a location separate from the vehicle operations areas. Visitor parking should also be separate from both employee parking lots and secure vehicle operations areas.

4.11.4 Identification Systems

A personnel and visitor identification system for both individuals and vehicles must be initiated to allow for positive identification of employees and visitors when entering secure areas of the facility. Postal personnel who are either career or contract employees should be provided with easily identifiable access card to permit entry into facilities. The Postal Security Unit or other postal managers should be responsible for the control, issuance and removal of employee, visitor and contractor identification badges.

A system should be in place to inspect and identify all vehicles prior to them entering any secure exterior operations area.

5. PERSONNEL SECURITY AND TRAINING

5.1 General

Of importance to postal operation and its personnel and as such it is fundamental to operators that any potential security risks that posed as a result of new employees or parties providing services entering into business, as well as those resulting from the redeployment of employees onto roles with different vetting or training requirements are minimized. Personnel security and training should be deployed to reduce and minimize security risks to the business, its customers, and employees.

5.2 Personnel Security Checks and Hiring Processes

5.2.1 The Recruitment and Selection policy must be documented for all employees working within the facilities of the DPO or handling mail at external locations.

- 5.2.2 The Recruitment and Selection policy must be consistent with national legislation to ensure prospective and current employees and contractors qualified to perform postal duties as a person of integrity.
- 5.2.3 The hiring process must include interviews, pre-employment data verification and other confirmation measures commensurate with positions or duties.
- 5.2.4 Career employees should be subjected to background screening (criminal history checks) consistent with applicable national legislations.
- 5.2.5 The postal services shall periodically review and evaluate personnel screening practices to determine if they are adequate and in compliance with accepted national standards. A random sampling of existing hires should be reviewed to ensure all designated procedures were followed.
- 5.2.4 The termination process shall be documented for all employees and contractors and to ensure with termination process the timely return of identification documents, access control devices, keys uniforms and other sensitive information.
- 5.2.5 A record system shall be maintained to prevent re-hiring of employees or contractors who have been terminated due to misconduct.

5.3 CONTRACTOR SECURITY REQUIREMENTS

- 5.3.1 Contractors used to perform mail handling/transport operations or other sensitive functions must initiate physical and personnel security measures as applied throughout the postal services. The contractor must conduct employee screening measures for all its employees handling mail and other related postal materials. The level of screening measures should be commensurate with the responsibilities of the contract personnel. The contractor should possess documented security processes and a documented business continuity plan. The contractor should also establish a reporting and communication process for employee performance and misconduct.



5.3.2 The contractor shall inform the DPO of any personnel findings or decisions which could pose potential security risk to the operation.

6. TRANSPORTATION AND CONVEYANCE SECURITY REQUIREMENTS FOR POSTAL SERVICES AND POSTAL CONTRACTORS

- 6.1 The postal services and authorized contractors should maintain the integrity and security of mail by all modes (air, highway, sea and rail) of transportation. The postal services should comply with all applicable national and international legislation regarding transportation standards.
- 6.2 Access to mail should be restricted as appropriate to postal employees or contractors with mail handling responsibilities.
- 6.3 Mail transport vehicles should be designed from resilient materials and possess features such as a solid-top, hard-sides or reinforced soft-sides and locked cargo doors. Vehicle should be inspected before loading and any signs of tempering reported.
- 6.4 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 must be secured (locked). The vehicle or means of conveyance must possess the ability to be secured (immobilized) when unattended unless it is located within secure postal or contractor premises.
- 6.5 Vehicles or conveyances should be clearly marked denoting that it is an authorized postal vehicle or postal contracted vehicle. Transport operators (postal or contractor) must be wearing a designated postal uniform and/or possess and clearly display a valid form of postal or contractor identification.
- 6.6 Vehicle cabin and ignition keys for all transport vehicles should be secured from unauthorized access. A key accountability process must be initiated.
- 6.7 Use of established measures to ensure postal network security through time and distance measurement of conveyance movement thereby enabling detection of route deviations. Routes, schedules and planned stops should be assessed for risk and if necessary additional security measures should be initiated to mitigate the risk.

7. TRANSPORTATION AND CONVEYANCE SECURITY REQUIREMENTS FOR POSTAL SERVICES AND FLEET CONTROLLERS

- 7.1 The postal services should ensure that the vehicles, conveyances, or containers are properly emptied at the beginning or end of daily use.
- 7.2 Period route and transport inspections should be conducted by Fleet controllers/ security personnel/ supervisors to ensure the designated procedures are followed.
- 7.3 Postal Services should perform security audits and inspections of staff / contractor facilities used to load, transport, or consolidate mail on regular basis.
- 7.4 Contractual agreements should be put in place to include a process for disciplinary action and/or contract termination for contract carrier violations.
- 7.5 To maintain transit time integrity the postal services management should detect and report unscheduled events (stops, delays, route deviations).

8. CUSTOMS PROCESSES

- 8.1 Postal Services must ensure that all international mail is made available for Customs review. Processes must be enforced to ensure the mail is presented as soon as possible to the national Customs entity.
- 8.2 The postal services must conduct quarterly meetings with customs to maintain an ongoing coordinated communication effort between Customs. The purpose of meetings is to discuss and resolve irregularities, volume availability profile and resource alignment.
- 8.3 Written procedures should be in place to ensure the respective Customs entity verifies the associated postal documents and seals on conveyances at ports of entry. A notification and reporting process should be in place to resolve irregularities.

8.4 The postal services should provide the necessary PREDES (PRE advice of international Despatch) information to Customs authorities daily.

9. AWARENESS & TRAINING MEASURES (MINIMUM SECURITY REQUIREMENT)

A security awareness training program must be maintained and documented for all employees and contractors.

10. POSTAL SECURITY UNIT FOR PREVENTION AND INVESTIGATIVE MANAGEMENT - OVERSIGHT

10.1 The policy will serve a guideline for security program covering the areas of prevention and investigation for the protection of mail, employees, partners, customers, and postal assets. (e.g., equipment, vehicles, uniforms, information technology, etc.)

10.2 The Chief Executive Officer will be the custodian of this policy. He or she will establish a dedicated Postal Security Unit or will appoint dedicated personnel in accordance with the Company Human Resources Policy and Procedures to perform safety and security measures. The personnel dedicated to these functions shall be commensurate with the size and operations of the administration.

10.3 The dedicated Postal Security Unit or dedicated security personnel should perform periodic facility and process security reviews.

11. POSTAL SECURITY UNIT FOR PREVENTION AND INVESTIGATIVE MANAGEMENT

11.1 The postal services shall utilize non-intrusive inspection technologies (e.g., X-ray, radiological, biological, etc.) based on a risk assessment.

11.2 The dedicated Postal Security Unit or dedicated security personnel shall have a security incident reporting system to track security incidents.

11.3 The postal security unit shall promote an incentive program for employees or other individuals to report suspicious activities including vulnerable procedures to create a deterrent environment and foster continuous improvement of security standards.

- 11.4 Sharing of best security practices through established communication channels such as the UPU Postal Security Group (PSG) or other regional security groups shall be allowable.

12. DISASTER RECOVERY, EMERGENCY PREPAREDNESS AND BUSINESS CONTINUITY PLANNING

- 12.1 The disaster recovery plan must be in place to ensure the security of mail, employees, and postal assets in the event of a man-made or natural disaster that would affect the flow of mail or postal operations.
- 12.2 The business Continuity Plan must be in place to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations.
- 12.3 A documented hazardous material response plan and or team for spillage procedures and/or handling dangerous goods must be in place.
- 12.4 Inter-agency cooperation and maintained comprehensive communication plan and for exchange of risk related information in support of ongoing operations (e.g., disasters and emergencies).

13. APPROVAL

- 13.1 The Board of Directors approves this policy. Once approved the Postal Security Unit will be established in accordance with the universal postal requirements.
- 13.2 The Job Description for a Postal Mail Security Officer will be developed and graded in consultation with the human resources department.
- 13.3 The approved policy will be circulated to all employees for implementation.