UPU status: **2**

Date of adoption at this status: **16 Feburary 2016**

Date of approval of this version: **16 February 2016**

Postal security – General security measures

UPU standards are updated in their entirety. Each update results in a new version, indicated by the version number following the number of the standard. Before using this document, please check in the Catalogue of UPU Standards that it is still valid. The Catalogue is freely available on the UPU website at www.upu.int.

Disclaimer

This document contains the latest information available at the time of publication. The Universal Postal Union offers no warrants, express or implied, regarding the accuracy, sufficiency, merchantability or fitness for any purpose of the information contained herein. Any use made thereof is entirely at the risk and for the account of the user.

Warning – intellectual property

The Universal Postal Union draws attention to the possibility that the implementation of this standard might involve the use of a claimed intellectual property right. Recipients of this document are invited to submit, with their comments, notification of any relevant rights of which they are aware and to provide supporting documentation.

As of the date of approval of this standard, the Universal Postal Union had not received such notice of any intellectual property which might be required to implement this standard, other than what is indicated in this publication. Nevertheless, the Universal Postal Union disowns any responsibility concerning the existence of intellectual property rights of third parties, embodied fully or partly, in this Universal Postal Union standard.

Universal Postal Union
Standards Programme
P.O. Box 312
3000 BERNE 15
SWITZERLAND
Tel: +41 31 350 3111
Fax: +41 31 350 3110
E-mail: standards@upu.int

Contents

Foreword

Postal services form part of the daily life of people all over the world. The Universal Postal Union (UPU) is the specialised agency of the United Nations that regulates the universal postal service. The postal services of its 192 member countries form the largest physical distribution network in the world. More than 5 million postal employees working in over 660 000 post offices all over the world handle an annual total of 434 billion letter-post items in the domestic service and 5,5 billion in the international service. More than 6 billion parcels are sent by post annually. Keeping pace with the changing communications market, postal operators are increasingly using new communication and information technologies to move beyond what is traditionally regarded as their core postal business. They are meeting higher customer expectations with an expanded range of products and value-added services.

Standards are important prerequisites for effective postal operations and for interconnecting the global network. The UPU's Standards Board develops and maintains a growing number of standards to improve the exchange of postal-related information between postal operators and promotes the compatibility of UPU and international postal initiatives. It works closely with postal handling organisations, customers, suppliers and other partners, including various international organisations. The Standards Board ensures that coherent standards are developed in areas such as electronic data interchange (EDI), mail encoding, postal forms and meters.

UPU standards are drafted in accordance with the rules set out in Part IV of the "General information on UPU standards" and are published by the UPU International Bureau in accordance with Part VI of that publication.

The UPU recognises that the safety and security of the postal sector is critical to support world-wide commerce, communication and safe transportation. To facilitate the development of security standards and recommended practices for adoption by designated postal operators, the UPU established the Postal Security Group (PSG).

The PSG is comprised of security experts from a number of UPU member countries and is charged with the development of global and regional security strategies to assist postal operators in their security missions. Through training initiatives, consulting missions and prevention programmes, the PSG strives to protect the employees and assets of the postal operators along with safeguarding the mails from fraud, theft and misuse.

This is the third version of the document. The change to the previous version, marked by a vertical bar in the margin, comprises a structural change to 5.2.2 (Access control systems for employees, visitors, service providers and vendors).

Introduction

One of the objectives of the Postal Security Group (PSG) is to enhance the security of all operations within the postal sector. The PSG in collaboration with other UPU stakeholders has defined a minimum set of security requirements, which can be applied to all facets of the sector. Developing measurable standards of security for the postal sector contributes to protecting postal employees and assets; protecting postal items in general; contributing to the security of the mode of transport used to carry mail items and enabling national and international authorities to apply risk assessment tools.

The physical and procedural security standards developed under the auspices of the PSG are applicable to critical facilities in the postal network. At the time of publishing, they are:

– S58, *Postal security standards – General security measures* (this document) defines the minimum physical and process security requirements applicable to critical facilities within the postal network;

– S59, *Postal security standards – Office of exchange and international airmail security* defines minimum requirements for securing operations relating to the transport of international mail.

NOTE In order to implement S59 as a requirement, S58 shall be implemented also. Only Regulated Agents, as defined by the International Civil Aviation Organization (ICAO) in Annex 17 to the Convention on International Civil Aviation, can conduct screening.

Postal security standards – Postal security – General security measures

1 Scope

This document defines the minimum physical and process security requirements applicable to critical facilities within the postal network.

NOTE It is incumbent upon the DOs to ensure compliance with respect to all domestic laws/legislation, regulations, etc.

DOs and postal supply chain parties can provide evidence that they comply with National Civil Aviation Security Program (NCASP) or internationally recognised security certification programmes deemed to comply with the requirements of UPU Standards S58 and S59.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, or references to a version number, only the edition cited applies. For undated references and where there is no reference to a version number, the latest edition of the referenced document (including any amendments) applies.

International Civil Aviation Organization, Technical Instructions for the Safe Transport of Dangerous Goods by Air (Doc 9284)

NOTE Requests for copies of ICAO publications should be submitted directly to ICAO's Document Sales Unit: sales@icao.int.

3 Terms and definitions

A number of common terms used in this document are defined in the UPU Standards glossary and in documents referred to in 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.

3.1
access control
in physical security, refers to the practice of restricting entrance to a property, a building, or a 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.

3.2
critical facility
office of exchange; air mail unit; postal facilities where aviation security screening is completed; the final postal facility where mail items transit prior to despatch via air

3.3
designated operator
any governmental or non-governmental entity officially designated by the member country to operate postal services and to fulfil the related obligations arising out of the Acts of the Union on its territory

3.4
minimum security requirement
technique, method, process or activity that consists of the minimum measures which shall be implemented to ensure secure operations within the critical facility with respect to local legislation, internal policy and procedures

3.5
screening
examination of mail by technical or other non-intrusive means that is intended to identify and/or detect explosives

3.6
single access system
physical characteristics of an access control system which restricts the entry of unauthorised individuals by only allowing one individual to enter through the controlled area before the entry door is closed. It shall prevent piggybacking or tailgating of employees without human intervention

NOTE This is usually accomplished through the use of turnstiles, but may also be accomplished through a pair of doors and specialty sensors.

4 Symbols and abbreviations

CCTV Closed Circuit Television System

DO Designated operator

ICAO International Civil Aviation Organization

NCASP National Civil Aviation Security Program

PSG Postal Security Group

5 Critical facility security standard

5.1 General information regarding physical security measures

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, CCTV and alarm/intrusion detection systems.

5.1.1 Risk assessment and critical facility security plans

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:

- critical facility design standards;
- perimeter barriers;
- perimeter windows, doors or other openings;
- lighting;
- locking mechanisms and key controls;
- access control measures.

5.1.2 Critical facility design standards

All critical facilities shall be constructed to national design standards for safety and security and contain resilient materials to preclude illegal entry.

A designated programme 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.

Restricted areas shall be easily identifiable, well-marked and secured with the appropriate access control measures.

5.1.3 Perimeter barriers

Physical barriers such as fencing, walls, and vehicle gates shall be installed to deny access of non-authorised individuals or vehicles onto 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.

5.1.4 Perimeter windows, doors or other openings

All exterior doors shall be of sufficient strength to prevent or delay forced entry by use of portable hand tools or other means of aggression.

The number of doors shall be the minimum necessary to provide adequate access and egress including emergency doors to the facility.

Signs and placards shall be placed on exterior doors denoting restricted access unless they cause a visible obstruction or local regulations do not allow. If appropriate, signs describing responsibility and procedures for notifying authorities should be readily visible if criminal events take place in the facility.

All exterior windows, doors and other openings shall be secured by appropriate locking mechanisms.

The facility risk assessment may indicate the need for additional security measures such as windows affixed with bars, mesh or any other material to harden these access points against unauthorised entry.

5.1.5 Lighting

Adequate lighting systems shall be installed in all pedestrian or vehicle entry/egress areas, exterior operations areas, parking areas, and along perimeter fences or walls. The lighting level shall illuminate these areas sufficiently to identify individuals or vehicles within close proximity. The inclusion of lighting in areas of close proximity to airports or runways shall be cognisant of aviation authority/airport requirements.

Where CCTV is used illuminating interior areas including operational storage areas shall be considered.

Emergency lighting shall be installed in critical operational areas.

5.1.6 Locking mechanisms and key controls

All lock mechanisms for pedestrian or vehicle entry/egress points shall be designed of hardened materials to prohibit access by non-authorised individuals.

A key control system shall be maintained for adequate key accountability.

The system shall register and record the issuance of keys and protects access to non-issued keys.

The key control system shall be administered by the Postal Security Unit or the respective postal facility manager.

5.2 Access control measures

5.2.1 General

Access control measures shall prevent unauthorised access to mail and mail conveyance vehicles in critical facilities. The appropriate level of access control shall be implemented at every critical facility to protect and secure postal assets.

NOTE Access control may 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. Access control measures may also consist of simple or complex electronic systems to verify and permit access to the secure areas. Regardless of the technological aspects of the methods utilised, 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. The access control system in a critical facility is segmented to ensure that employees, visitors, service providers and vendors be only permitted access to those areas of a facility where they have work functions or conduct business.

5.2.2 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 facilities. It may consist of one or a combination of the following:

i a manual access control system:

- a uniformed security guards, a receptionist or other personnel staff shall be at entry/egress points to verify the entry privileges for each individual;
- b 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;
- d a registration system shall be maintained to record entries of non-employees into secure areas of the critical facility;

ii an automated (electronic) access control system.

NOTE 1 The carriage of personal belongings, e.g. bags, and the limitation thereof as well as the institution of search procedures should be considered.

The system shall be designed to prohibit unauthorised entries of individuals through the entry/egress 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.

NOTE 2 A single access system can also be accomplished by assigning a 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 should be used;

A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility.

5.2.3 Access control systems for vehicles

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 unauthorised vehicles do not gain access into the secure exterior operations area.

If it is necessary for a non-official or third party 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.

5.2.4 Identification systems

A personnel and visitor identification system shall be implemented to allow for positive 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, photograph and expiration date. Other information such as access level, department/unit, may be added as required by local regulations and legislation.

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.

A system shall be put in place to inspect and identify all vehicles prior to them entering any secure exterior operations areas.

6 Personnel security and training

6.1 General

Important to postal operations are its personnel and as such it is fundamental to operators that any potential security risks that are posed as a result of new employees or parties providing services entering into the business, as well as those resulting from the redeployment of employees onto roles with different vetting or training requirements are minimised. Personnel security and training shall be deployed in order to reduce and minimise security risks to the business, it customers and employees.

6.2 Personnel security and hiring processes

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 checks (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 confirmation measures commensurate with positions or duties.

The termination process shall be documented for employees and contractors.

The termination process shall 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 employees or contractors who have been terminated due to misconduct.

6.3 Contractor security requirements

Contractors used to perform mail handling/transport operations or other sensitive functions shall apply personnel security measures equivalent to the DOs as described in 6.2.

The contractor shall inform the DO of any personnel findings or decisions which could pose potential security risks to the operation.

6.4 Awareness and training measures

Security awareness training programmes shall be documented and maintained for all employees and contractors.

7 Transportation and conveyance security requirements for DO's and postal contractors

The DO and authorised contractors shall document processes and procedures for security of the mail by all modes (air, road, sea and rail) of transportation. The DO 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. Vehicles should be inspected before loading and any signs of tampering reported.

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).

Whenever possible, vehicles or conveyances shall be clearly marked or identifiable as an authorised postal vehicle or postal contracted vehicle.

Whenever possible, 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 unauthorised access.

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.

8 Compliance audit programme and oversight

An annual compliance audit shall be conducted by personnel independent of the critical facility management team.

The individuals conducting the compliance audit review shall be afforded the necessary authority to obtain relevant information and to enforce corrective action.

The compliance audit review programme covers the entire mail security programme to ensure implementation of security requirements. The compliance audit review programme shall include, but not be limited to, an emphasised focus on:

- facility security;
- personnel security;
- transportation and conveyance security.

The DO shall ensure that the management of the compliance audit review programme is independent from individuals responsible for the implementation of security requirements.

Records of the compliance audits and recommendations shall be maintained.

The result of the compliance audits shall be reported to the executive management of the DO. Follow-up actions shall be monitored and documented.

9 Postal security unit for prevention and investigative management

9.1 Postal security unit for prevention and investigative management (minimum security requirement)

The DO shall have a documented security programme 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.

EXAMPLE Equipment, vehicles, uniforms, information technology, etc.

The DO 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 DO.

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

9.2 Disaster recovery, emergency preparedness and business continuity planning

The DO shall document and communicate to appropriate employees:

- a 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;
- a business continuity plan to minimize postal interruption in the event of significant incident which might impact domestic or international postal operations.

Bibliography

This bibliography provides full reference and sourcing information for all standards and other reference sources which are quoted in the above text. For references which mention specific version numbers or dates, subsequent amendments to, or revisions of, any of these publications might not be relevant. However, users of this document are encouraged to investigate the existence and applicability of more recent editions. For references without date or version number, the latest edition of the document referred to applies. It is stressed that only referenced documents are listed here.

[1] International Civil Aviation Organization, Annex 17 to the Convention on International Civil Aviation: Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference

NOTE Requests for copies of ICAO publications should be submitted directly to ICAO's Document Sales Unit: sales@icao.int.