BS 7499:2013

BSI Standards Publication

Static site guarding and mobile patrol service – Code of practice

bsi.

...making excellence a habit.™

Publishing and copyright information

Published by BSI Standards Limited 2013

ISBN 978 0 580 81340 5

ICS 13.310

The following BSI references relate to the work on this standard:
Committee reference GW/3
Draft for comment 13/30275054 DC

Publication history

First published as BS 7499-1, December 1991

Second edition, June 1998

Third edition, February 2002

Fourth edition, July 2007

Fifth (present) edition, September 2013

Amendments issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 26, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 September 2013. It was prepared by Technical Committee GW/3, *Manned security services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 7499:2007, which is withdrawn.

Information about this document

This is a full revision of the standard and has been updated to reflect changes in current working practices, including the use of short term lease/hire vehicles.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

It has been assumed in the preparation of this British Standard that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific regulations:

- Rehabilitation of Offenders Act, 1974 [1];
- The Working Time Regulation, 2003 [2];
- The Equality Act, 2010 [3];
- Private Security Industry Act, 2001 [4];

- Data Protection Act, 1998 [5];
- Health and Safety at Work etc. Act, 1974 [6].

This page deliberately left blank

1 Scope

This British Standard gives recommendations for the management, staffing and operation of an organization providing security guarding (see Annex A) services on a static site and/or mobile patrol basis.

This British Standard does not apply to all security services, for example cash-in-transit services, secure parcel services, keyholding and response services, door supervisors, close protection services, event stewarding and the management and operation of closed-circuit television (CCTV).

NOTE Recommendations for cash-in-transit services, CCTV, door supervisors, keyholding and response services and event stewarding are given in BS 7872, BS 7958, BS 7960, BS 7984 and BS 8406 respectively.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 5839-1, *Fire detection and fire alarm systems for buildings – Part 1: Code of practice for design, installation, commissioning and maintenance of systems in non-domestic premises*

BS 5979, *Remote centres receiving signals from fire and security systems – Code of practice*

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS 7958, *Closed circuit television (CCTV) – Management and operation – Code of practice*

BS 7984, *Keyholding and response services – Code of practice*

BS EN 50131-1, *Alarm systems – Intrusion and hold-up systems – System requirements*

PD 6662, *Scheme for the application of European standards for intrusion and hold-up alarm systems*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 assignment instructions
operational document detailing site specific contractual duties

3.2 check call
routine communication to verify the location and status of a security officer on an assignment

3.3 competent person
person, suitably trained and qualified by knowledge and practical experience, and provided with the necessary instructions, to enable the required task(s) to be carried out correctly

3.4 control room
location where operational procedures are monitored and/or managed

NOTE For the purposes of this British Standard the control room is also known as the communication centre.

3.5 controller
person designated to monitor control room operations and communications

3.6 customer
individual or body retaining the services of the organization

3.7 key(s)
instrument or data allowing authorized access to a customer's property

3.8 keyholding
service whereby the organization holds keys to a customer's premises and/or equipment for use as agreed in the contract

NOTE 1 Keyholding might involve dual key systems. One key is held by the customer, and another (different) key to the same premises or equipment is held by the organization. Both keys would be required to gain access to the premises or to operate the equipment.

NOTE 2 See BS 7984 for further information on keyholding and response services.

3.9 mobile patrol
security services provided by security officers travelling to multiple sites physically distant from one another, within a defined period of time

3.10 organization
sole or main provider of static site guarding and/or mobile patrol services to a particular customer

3.11 principal
owner, partner, board director or other top executive in the private sector, or an executive officer in the public sector or a not-for-profit organization

3.12 secure facility
strongly constructed dedicated room or securely mounted lockable cabinet for the holding of keys

3.13 security officer
person who performs duties at a static site or on a mobile patrol

3.14 static site
fixed location or premises to which a security officer is assigned for a fixed length of time

3.15 supplier
individual or company (and the persons employed, including all levels of subcontractor, by that individual or company) that supplies the organization with equipment, material and/or labour which is used in providing the service to the customer

3.16 takeover
transfer of contractual responsibilities from one organization to another

4 The organization

4.1 Structure

The organization should possess a clearly defined management structure showing control and accountability at each level of operation.

The organization should operate a complaints management system.

NOTE 1 Guidance is given in BS ISO 10002.

Details of the ownership of the organization should be established and the principals' curricula vitae made available. Any unspent criminal convictions or undischarged bankruptcy of a principal should be disclosed on request.

NOTE 2 Attention is drawn to the Rehabilitation of Offenders Act 1974 [1], whose provisions govern such disclosure.

4.2 Finances

The organization should have sufficient working capital for its requirements. The capital reserves of the organization should be sufficient for current and planned needs.

The organization should be able to present two years' audited trading accounts, except if it is starting as a subsidiary of an established business, and adequate financial backing is evident, or in the case of a new start up business where management accounts should be made available to show that the organization can demonstrate it has the funding available to achieve its plan for the business.

NOTE Where the organization is solely providing a service in-house (and not contracting out such services), some of the recommendations given in this subclause might not apply.

The organization should prepare annual accounts in accordance with applicable accounting standards. The accounts should be certified by an accountant or solicitor with complete details of expenditure and income. Accounts should be available for examination on request.

4.3 Insurance

The organization should possess insurance cover commensurate with the business undertaken and the number of persons employed, e.g. public liability, contractual, efficacy, employer's liability and vehicle insurance.

NOTE Where the organization is solely providing a service in-house (and not contracting out such services), then efficacy insurance and some other types of insurance mentioned in this subclause might not be needed.

Fidelity guarantee should be available up to limits required by the customer, e.g. loss of keys, wrongful arrest and product liability.

5 Resources

5.1 Premises

The organization should have an administrative office(s) and/or operational centre(s) where records, professional and business documents, certificates, correspondence, files and other documents necessary for conducting business transactions should be kept in a secure manner. The location of records and documentation, both local and centralized, should be clearly defined by the organization.

5.2 Control room

5.2.1 Design

Control rooms should be designed to allow the following functions, whether in combination or alone, to be performed:

a) provision or procurement of assistance, information or advice for security officers (on static sites and mobile patrols) and supervisors, in routine and emergency situations;

b) effective monitoring of security officers (on static sites and mobile patrols) and supervisors, by strict observance of documented, established telephone, radio or other communication procedures;

c) recording, in accordance with **5.2.7**, of all appropriate routine and emergency matters, to enable management to deal quickly and efficiently with contractual responsibilities;

d) recording the movement of customers' keys held in the control room (see **6.6**).

Control rooms should be restricted areas open only to authorized personnel.

Where control rooms are outsourced, the organization should be provided with documentation that the control room conforms to **5.2**.

5.2.2 Location

Control rooms should be situated within premises owned or leased by the organization, and to which the organization has access at all times.

5.2.3 Construction

All parts of the shell of a control room should be soundly constructed to ensure physical security, safety and integrity, for the protection of employees and the safeguarding of customers' records and property.

Only the following openings should be permitted in the shell of a control room:

a) a normal entrance;

b) emergency exits;

c) glazed areas;

d) ventilation inlets and outlets;

e) service inlets and outlets;

f) key transfer hatches.

NOTE Attention is drawn to relevant building regulations, fire regulations and health and safety legislation.

If the normal entrance is directly accessible from the exterior of the premises in which the control room is situated, it should comprise two sequential doors controlled from within the control room and interlocked to prevent more than one door from opening at a time.

If the normal entrance to the control room is located within the premises to which access is controlled, a single door should be sufficient. The door should open outwards and should have a locking device, operable from within the control room and which can be unlocked from outside.

All doors, including emergency exits, hinges, frames, fixings and locking devices should be of substantial construction, resistant to entry by physical attack.

Emergency exit doors should open outwards and should have unlocking devices for release, only in emergencies. Emergency doors should be fitted with a 24 hour remote-signalling intruder alarm system conforming to BS EN 50131-1/PD 6662.

Voice communication across normal entrance doors should be by an intercom system. A viewing means should be incorporated so that the identity of persons wishing to enter the control room can be established before the control room door is opened.

External or publicly accessible glazed areas should be protected to offer resistance to entry by physical attack, e.g. by the use of window bars. Ventilation and service inlets and outlets should also be protected. Internal operational areas should not be visible externally.

The equipment, furnishings and layout of the control room should allow its efficient operation. Heating, lighting and ventilation should be provided to ensure a comfortable working environment.

Facilities for the management and operation of CCTV systems should conform to BS 7958.

Control rooms that serve as a manned or unmanned alarm-receiving centre for intruder, fire, CCTV and social alarm systems and other monitoring services, and require a unique reference number (URN) for emergency response, should be constructed and secured in accordance with BS 5979. [1)]

5.2.4 Facilities

A deliberately operated remote-signalling alarm system conforming to BS EN 50131-1/PD 6662 should be installed, with sufficient deliberately operated devices to allow the controller to warn of any attack on the control room.

The control room and surrounding areas should be fitted with a fire alarm system, designed and installed in accordance with BS 5839-1.

Single-manned control rooms should be fitted with a remote-signalling fail-safe emergency alarm system, which should warn whether the controller is disabled for more than 60 minutes. This system should activate an alarm at another remote 24 hour control room or an alarm receiving centre constructed and equipped in accordance with BS 5979.

Emergency lighting should be provided, able to start up within 60 seconds of failure of mains powered illumination. Emergency lighting should be able to illuminate the control room for continued operation and should provide at least 3 hours continuous operation.

Where computerized and/or electronic systems are in operation, adequate resources should be available to ensure continued operation of the control room in the event of power or system failure.

Where customer keys are held, strongly constructed, secure, lockable storage should be provided for keys.

A communication line exclusive to the control room should be provided. Where possible, the line should be routed separately from other lines into the premises. An emergency alternative means of communication should be provided.

[1)] pr EN 50518-1, pr EN 50518-2 and pr EN 50518-3 are to replace BS 5979 for alarm receiving centre (ARC) requirements for intruder alarm systems in 2014.

5.2.5 Procedures

Controllers should receive, in writing, details of the identity of the person to whom they should report and the method of reporting incidents or problems both within the organization and to the customer.

The organization should review and update control room information at regular intervals (at least once every 12 months).

A control room manual should be produced for the guidance of controllers. The manual should clearly indicate the stages at which an incident should be reported by the controller to more senior personnel. A copy of the control room manual should be readily available within the control room at all times.

The control room manual should outline the action to be taken on receipt of incident reports, and methods of recording incidents. Records of incidents should include the following:

a) the date, time and location of the incident;

b) the date and time of reporting, who reported and who received the report;

c) details of the incident;

d) action taken, including onward reporting;

e) action to be taken;

f) names and addresses of persons who witnessed the incident.

Check calls from security officers should be received and recorded at the control room at intervals specified in their assignment instructions. The control room manual should detail the procedures to follow and actions to be taken in the event of a late and missed check call. The frequency of check calls should be determined following a health and safety risk assessment, and should take into account the number of security officers on duty. Procedures for daily verification that automated systems are working should be detailed in the control room manual and verifications should be documented.

5.2.6 Information

The controller should have immediate access to the following:

a) all assignment instructions,

b) details of hours of cover for all assignments with the number of security officers, the number of contracted visits, and site telephone numbers;

c) a means of displaying the names of security officers working at each assignment during shifts;

d) the names, addresses and telephone numbers of all security officers, including supervisors and principals of the organization;

e) emergency contact records (including telephone numbers) for all customers;

f) telephone numbers of police stations within the operational area of the control room;

g) useful telephone numbers (e.g. water companies, electricity companies, boarding-up services);

h) a copy of the control room manual;

i) emergency procedures and contingency plans in case of fire, flood or bomb threat, etc., for the control room and other premises;

j) a register of keys that are held in the control room.

5.2.7 Records

NOTE Minimum periods for retention of records might be reviewed, if applicable, for particular purposes, especially with regard to potential liabilities for civil action.

The following records should be kept:

a) records of all reported incidents for a minimum of 12 months from the date of the event. Entries should be numbered serially and should include the time and date of the incident and the name of the controller completing the record;

b) records of all telephone and radio calls from security officers and supervisors for a minimum of 12 months.

Details of all check calls should be recorded, including missed and late check calls. Precise times of contact should be noted.

Records should be made of all mobile patrol visits and supervisory visits.

Controllers should also maintain a register of keys held in the control room and should sign for keys on shift change over.

5.2.8 Personnel

The number of controllers on duty should be consistent with the expected workload.

Toilet and washing facilities and a facility for cooking or heating food or drink should be provided within close proximity of the control room and within the protected confines of the premises in which the control room is located.

A first-aid box and fire-fighting equipment should be provided.

5.3 Staff

5.3.1 General

The organization should ensure that it has employed sufficient security officers to fulfil its contractual obligations and sufficient supervisory staff to manage day and night assignments and to make regular site visits.

5.3.2 Selection and screening

All persons undertaking, or having access to details of, security duties, should be selected and screened in accordance with BS 7858.

If employees are acquired through a takeover, the organization should satisfy itself that the recommendations of this subclause have been fully met.

Prospective employees should be asked to demonstrate good reading, writing and verbal communication abilities.

Where night-time working is involved, prospective employees should be asked to confirm that there is nothing in their circumstances that would be detrimental to their working night shifts. Night-time workers should be offered the opportunity of a free medical assessment.

NOTE Attention is drawn to the Working Time Regulation 2003 [2].

Employers should validate the employees driving license against company policy for those employee's whose duties involve driving. The employer should hold on file a validated copy of the employee's driving licence. The employer should check the employee's driving licence or carry out a DVLA license check on the employee every six months.

5.3.3 Health

Prospective employees should be sent an employment medical questionnaire, with questions that relate to, or are intrinsic to, the job function, this can be sent with the offer of employment.

NOTE 1 The offer of employment is conditional on the results of the medical questionnaire supplied, which might fundamentally inhibit the employee from carring out the job.

NOTE 2 Attention is drawn to the Equality Act 2010 [3].

In order to ensure that the physical condition of security officers remains compatible with the duties to which they have been assigned, documented procedures should be in place for performing routine health checks and reports. When the physical demands of a person's duties change their physical condition and suitability should be reassessed as appropriate.

NOTE 3 Where health and safety risk or medical concerns of personnel are raised, it is reasonable for a company to ask that person to undergo a medical examination to ensure fitness for duty.

5.3.4 Terms and conditions of employment

Employees should be sent a written statement of the terms and conditions of their employment that include details of the following:

a) job title;

b) effective start date;

c) probationary period (if required);

d) provisional period subject to screening (if applicable);

e) pay and allowances;

f) hours and days of work;

g) leave entitlement;

h) conditions of payment during absence through illness;

i) pension entitlement;

j) industrial injury procedures;

k) the address of the organization;

l) equipment supplied;

m) disciplinary and appeals procedures;

n) terms of notice of termination of employment.

Employees should not be required to work hours that could be detrimental to their health, safety or efficiency.

NOTE Attention is drawn to statutory requirements relating to employment, and in particular, to requirements relating to working hours.

5.3.5 Disciplinary code

Employees should be instructed that the following (including the aiding and abetting of others) could constitute a breach of the terms and conditions of employment:

a) neglecting to complete a required task at work promptly and diligently, without sufficient cause;

b) leaving a place of work without permission, or without sufficient cause;

c) making or signing any false statements, of any description;

d) destroying, altering or erasing documents, records or electronic data without permission or through negligence;

e) divulging matters confidential to the organization or customer, either past or present, without permission;

f) soliciting or receipt of gratuities or other consideration from any person;

g) failure to account for keys, money or property received in connection with business;

h) incivility to persons encountered in the course of duties, or misuse of authority in connection with business;

i) conduct in a manner likely to bring discredit to the organization, customer or a fellow employee;

j) use of uniform, equipment or identification without permission;

k) reporting for duty under the influence of alcohol or restricted drugs, or use of these whilst on duty;

l) failure to notify the employer immediately of any:

   1) conviction for a criminal and/or motoring offence;

   2) indictment for any offence;

   3) police caution;

   4) legal summons;

   5) refusal, suspension or withdrawal (revocation) of a licence.

      NOTE 1 An example of such a licence would be a Security Industry Authority (SIA) licence. For definitions see the SIA website.

m) permitting unauthorized access to a customer's premises;

n) carrying of equipment not issued as essential to an employee's duties, or use of a customer's equipment or facilities without permission;

o) not maintaining agreed standards of appearance and deportment whilst at work.

NOTE 2 This list is not exhaustive and does not necessarily include all actions within a company policy that could or could not also constitute criminal offences.

5.3.6 Identification

Employees, who are required to be screened in accordance with **5.3.2**, should be issued with an identity card incorporating the following information:

a) the name, address and telephone number of the organization;

b) the name of the employee, employee number and employee's signature;

c) the expiry date of the card (not more than three years from the date of issue);

d) a current photograph of the employee.

Employers should require that employees carry their identity cards whilst on duty.

Identity cards should be formally withdrawn from employees renewing their cards or leaving the organization, and destroyed in a secure manner.

A record of identity cards issued should be maintained. This record should also indicate the status and location of withdrawn cards, e.g. whether they have been destroyed or lost, or where they are held by the employee/organization.

NOTE Where a security officer is required to display a SIA licence this does not negate the need for company identification.

5.4 Equipment and uniforms

5.4.1 Uniform

Unless otherwise requested by the customer, employees should be supplied with a uniform to wear when on duty. Employee uniforms should clearly display the insignia of the organization. Uniforms should be readily distinguishable from those of the civil emergency services or armed forces.

Some clothing, such as a high visibility jacket, should be available to employees for use on occasion, whether or not the employee is in uniform and is required to respond to an emergency call. This clothing should enable the employee to be clearly distinguished by the civil emergency services or armed forces.

The organization should ensure that uniforms are periodically cleaned and renewed.

5.4.2 Vehicles

5.4.2.1 General

Unless they are involved in covert operations or otherwise excepted under contract, operational vehicles should clearly display the organization's name, badge or logo, and telephone number. Operational vehicles should:

a) be appropriate for the intended use;

b) carry a two-way communication device;

c) be inspected by the organization at least once per month to ensure that they are roadworthy;

d) be serviced regularly, in accordance with the manufacturer's instructions;

e) have any damage repaired as soon as possible;

f) be kept clean and tidy.

5.4.2.2 Vehicles carrying keys

Where an operational vehicle is required for keyholding and alarm response, the response should be carried out in accordance with BS 7984.

Where the operational vehicle is solely for mobile patrolling, keys should be kept in the possession of security officer(s) throughout the period of use or securely contained within a safe secured in the vehicle.

Where short term lease/hire arrangements render it impractical to secure a safe to the vehicle, companies should deploy an additional security officer to remain with the unsecured keys for the duration of the patrol.

Where physical conditions permit, the safe should be located within a compartment within the body of the vehicle. This compartment should be separately locked and should have no glazed or removable panels.

Where this is not possible, the safe should be located so that it cannot be seen externally.

Adequate locks should be fitted to the vehicle and/or the compartment within which the safe is held. Where possible, access to the safe should be only from within the vehicle.

The vehicle should be fitted with an alarm and an immobilizer.

It should be possible for the control room to ascertain the destination or location of the vehicle at all times.

NOTE For example, the vehicle's location can be monitored by fitting a tracking device, or a GPS signal.

Where a tracking device is installed in the vehicle, it should be able to signal the location of the vehicle to a remote 24 hour monitoring centre. The tracking system should be known to cover the entire area in which the vehicle operates.

5.4.3 Other equipment

All equipment used by employees or supplied to a customer should be appropriate for the intended use, in good working order and maintained regularly.

Timing devices should be regularly calibrated (see **5.4.4**).

5.4.4 Equipment records

Records should be kept of all equipment issued. Employers should require employees to sign for equipment and uniforms received, and to give an undertaking to return equipment on termination of employment.

Records of equipment calibrated and/or repaired should be kept and maintained for at least 12 months.

Records of vehicle maintenance and repair should be kept for the period of ownership of the vehicle or for longer if there has been an accident and a claim has been made.

5.5 Training

5.5.1 General

The organization should have a clearly defined and documented training policy.

5.5.2 Induction training

NOTE The content, timing and duration of induction training are left to the discretion of the organization.

The organization should provide induction training in matters related to conditions of employment and organizational procedures for all employees. This induction training should be additional to the basic job training described in **5.5.3**. Induction training should be completed before the security officer is appointed to an assignment.

5.5.3 Basic job training

Basic job training should be provided for all employees engaged in security duties, whether full-time or part-time, including seasonal and casual employees.

*NOTE 1 This training can be waived for new employees with industry experience who possess an appropriate qualification in a security discipline that is comparable with that issued by the Sector Skills Body (SSB) (see **5.5.8**).*

NOTE 2 SIA licensing requirements apply if working in licensable security activity. A person falling within the definition of licensable conduct under the Private Security Industry Act 2001 [4] is required to be licensed in accordance with that Act.

Basic job training should be provided prior to commencement of operational duties. Training should be provided by competent, qualified training persons, in a room that is suitable for the purpose of training. The room should be adequately equipped and conducive to effective learning.

Training should last a total of at least 32 hours, including the examinations, and should cover the following core subjects:

a) introduction to the security industry role and responsibilities of security officers;

b) patrolling;

c) access control;

d) searching;

e) security and emergency systems;

f) fire safety;

g) health and safety at work;

h) the law;

i) emergencies;

j) customer care and social skills;

k) communications and reporting;

l) equality and diversity;

m) communication skills and conflict management.

When the training period is complete, the trainee should take a written examination with a national recognized qualification that meets the minimum core competency as set by the Sector Skills Body (SSB).

The employer should carry out a gap analysis for security personnel holding a door supervision license (including those who have transitioned from a door supervising license to security guarding) or close protection license who wish to work in the security guarding area. Any training identified by the gap analysis should be provided.

The training should also include additional training hours for subject-specific modules that relate to the role to be undertaken, for example:

1) retail duties;

2) crowd control;

3) reception skills;

4) use of technology.

5.5.4 Assignment-specific training

New employees on a first assignment, or employees transferring between assignments, should be given on-the-job training appropriate to the assignment and to the needs of the trainee and the customer. For a period that reflects the complexity of the assignment (not normally less than 8 hours), a newly appointed security officer should be supernumerary whilst becoming familiar with the site requirement. This period should also reflect the site shift pattern, encompassing both day and night shifts if appropriate.

During the first three months of employment, either on a first assignment or for employees transferring between assignments, the competence of the security officer should be assessed by a suitably qualified or experienced supervisor or manager against performance criteria comparable with the core competencies as defined by the SSB.

5.5.5 Control room training

Training and instruction of controllers should include the following:

a) outline of control room operations;

b) detailed explanation of duties;

c) radio and telephone procedures;

d) documentation and recording procedures;

e) emergency procedures;

f) location and use of control room records;

g) explanation of security officers' rosters;

h) explanation of controllers' rosters.

The competency of the controllers should be assessed and any remedial training undertaken if required. Training records should be maintained.

5.5.6 Supervisory training

Employees who have supervisory responsibilities should be trained to a proficient standard by suitably qualified and experienced persons. Training should be provided in the following areas:

a) the role of a supervisor;

b) team behaviour;

c) leadership;

d) decision making;

e) problem solving;

f) communication skills;

g) performance review;

h) time management;

i) customer service.

In addition, supervisors should be encouraged to improve their level of knowledge in the following areas:

1) health and safety at work;

2) the protection of premises and property;

3) electronic security;

4) law;

5) arrest procedures;

6) contingency planning;

7) disaster recovery.

The competency of the supervisors should be assessed and any remedial training undertaken if required. Training records should be maintained.

5.5.7 Specialist training

Security officers engaged to perform specialist duties (e.g. first aid, fire-fighting, airport security, lift rescue) should be trained to a proficient standard by suitably qualified persons. Training should be provided on the use of specialized equipment.

5.5.8 Training exemption and transferability of qualifications

Exemption from basic job training is at the discretion of the organization. However, regardless of their qualifications, employees new to the organization should not be exempted from basic job training following a break from employment in the security industry of six months or more.

Employees new to the organization with industry experience should not be exempt from the induction training described in **5.5.2**.

NOTE SIA licensing requirements apply if working in licensable security activity. A person falling within the definition of providing licensable conduct under the Private Security Industry Act 2001 [4] is required to be licensed in accordance with that Act.

5.5.9 Takeovers

If employees are acquired through a takeover, the organization should identify their training needs and address them with a specific training policy. This policy should take practical work-related experience as well as qualifications into account.

Employees acquired through takeover should not be exempt from the induction training given in **5.5.2**.

5.5.10 Refresher training

The effectiveness of all security officers should be monitored and, if necessary, refresher or remedial training should be provided by suitably qualified persons as soon as practicable.

5.5.11 Contingency training

If there is a change in methods, procedures or legislation, security officers should be retrained to a proficient level by suitably qualified personnel. If practicable, training should take place before change is implemented.

5.5.12 Vocational training

All employees engaged in security and mobile patrol activities should be encouraged to achieve recognized formal qualifications, in addition to basic job training, in security disciplines, e.g. qualifications based on the appropriate national occupational standards.

5.5.13 Training records

All training provided online should be recorded electronically. All other training should be signed by the trainee, countersigned by the trainer and retained.

Where a certificate of training is provided by a recognized and relative sector competent training organization, a copy should be retained.

5.6 Suppliers

5.6.1 Suppliers of subcontract labour

The organization should obtain the customer's agreement on conditions for the use of suppliers of subcontract labour for undertaking the duties of security officers, supervisors and controllers.

Employers should require that employees of subcontract labour also follow the recommendations given in **5.3**, **5.4** and **5.5**. The organization should satisfy itself that these recommendations have been followed.

NOTE Attention is drawn to HMRC guidance on use of labour providers.

5.6.2 Qualifications of suppliers' personnel

The organization should satisfy itself that suppliers' personnel who have access to a customer's site and/or confidential records:

a) are satisfactorily screened in accordance with BS 7858;

b) are satisfactorily experienced and/or trained to undertake the work involved;

c) are adequately insured;

d) have individually signed a confidentiality agreement relating to the disclosure of the customer's and the organization's confidential information and/or material;

e) agree to report immediately to the organization any alleged or actual contravention of the law;

f) are appropriately licensed by the SIA.

Evidence of items a) to f) above should be retained by the organization.

5.7 Documents and data

Separate records (hardcopy or electronic) should be maintained for each customer, employee and supplier.

The records should be held in a secure manner, but should be easily accessible to authorized persons who have been screened (see **5.3.2**).

NOTE 1 Attention is drawn to the Data Protection Act 1998 [5].

Amended and/or updated records should be identifiable by date and clearly distinguishable from previous versions.

Information stored in an electronic retrieval system should be regularly backed-up. The back-up copies should be stored separately.

NOTE 2 Further information on the management of electronic data can be found in BS ISO/IEC 27001 and BS 7799-1. Advice on the storage of electronic media can be found in PD 5454.

Archived records should be clearly indexed.

All records concerning a contract should be maintained for at least 12 months after termination of the contract. Such records should include:

a) all issues of assignment instructions;

b) daily registers and patrol and incident reports;

c) details of persons employed on the assignment.

An employee's basic records (as detailed in BS 7858) should be kept for at least 7 years from the cessation of their employment.

NOTE 3 Minimum periods for retention of records can be reviewed if applicable for particular purposes, especially with regard to potential liabilities for civil action.

6 Service

6.1 Sale of services

6.1.1 Contacting prospective customers

When contacting potential customers in order to promote security services, confirmation of the identity of the individual representing the organization and the organization being represented should be given and the purpose of the contact made clear. Enquiries should not be made of their existing operational security arrangements (i.e. sensitive information) however general service requirements can be ascertained.

6.1.2 Customer information

Organizations should provide potential customers with the following basic information, which might take the form of a brochure:

a) the name, address(es) and telephone number(s) of the organization;

b) the name(s) of the principal(s) of the organization and contact name(s) for further information;

c) details of uniforms and equipment, and identifying insignia;

d) details of the communication systems used by personnel on duty.

Where the following items apply to the organization, this information should also be provided:

1) details of trade association membership, claims of compliance with industry standards, and/or details of certification by a UKAS-accredited (United Kingdom Accreditation Service) certification body and SIA Approved Contractor Scheme status;

2) the registered number, address and date of registration, if the organization is an incorporated company;

3) any previous name(s) of the organization;

4) the details of any parent organization (e.g. immediate holding company or ultimate holding company).

If requested by a potential customer, the organization should supply additional information as follows:

i) terms and conditions of employment of a security officer on guarding duties;

NOTE Terms and conditions of employment might include the average hourly rate of pay and the maximum number of hours in a typical working week.

ii) the type and extent of insurance cover;

iii) reference sources for details of previous or current work carried out by the organization;

iv) an organization chart and details of the number of employees, employee qualifications and number of personnel on supervisory duties alone.

6.1.3 Quotations

A clear quotation should be provided by the organization. If the quotation is accepted by the customer, it should form part of the contract. The quotation document should state:

a) the terms and conditions under which the work would be carried out;

b) the total costing for the service, and the arrangements for payment;

NOTE 1 Costing can include information on the gross pay of personnel.

c) the contract period, along with procedures for termination of the contract and reference to any exclusion, penalty clauses or other restrictions;

NOTE 2 The contract might not necessarily be for a specified period, but can take the form of a temporary works order.

d) the liabilities of the organization, which should not be unlimited, other than by law;

e) details of the customer's requirements, derived from an initial site inspection (see **6.2**) or from the customer's written instructions, and including clear cross-reference to any separately documented requirements or instructions;

f) arrangements for statutory holidays;

g) the obligations of the organization to the customer, including any provision of specialist advice or duties, and reference to any relevant British Standards;

h) the obligation of the organization to maintain confidentiality with respect to information obtained whilst tendering for or fulfilling a contract;

i) that the organization cannot enter into any commitment which would involve assuming the powers of the civil police;

j) the obligation of the customer to identify and consult with the organization on any specific health and safety requirements that apply, or are likely to apply, during the period of the contract;

k) the obligation of the customer to provide and/or maintain any specified item or service, which the customer has agreed to provide and which is necessary for fulfilling the assignment.

6.1.4 Quotations for mobile patrol services

In addition to the items listed in **6.1.3**, quotations for mobile patrol services should:

a) include an undertaking that keys are immediately surrendered to an authorized representative of the customer if requested by the customer in writing;

b) state the period of retention and method of disposal of any keys that are unclaimed on cessation of a contract;

c) state that mobile patrol services might be provided simultaneously for a number of customers, and that, accordingly, interruptions or delays can arise if an incident occurs at the premises of another customer during the course of a patrol officer's round of duty.

6.1.5 Contracts

The customer should be asked to sign either:

a) a form of acceptance indicating that they have read and understood the quotation, terms and conditions; or

b) a contract document referring to the quotation, terms and conditions.

The contract should be agreed and exchanged before work commences, or, in cases of great urgency, as soon as practicable.

If the customer is reluctant to enter into a written contract, a copy of the quotation, terms and conditions should be sent to the customer with a letter stating that, in the absence of indication to the contrary, the terms and conditions of the organization apply to the work.

If the quotation, terms and conditions are accepted but include amendments or optional extras, the organization should confirm in writing the agreed changes within seven days.

6.1.6 Contract records

Copies of records relating to the contractual agreement between the customer and the organization should be retained in a customer file. These records should include pre-contract documentation, site inspection reports, agreed assignment instructions, receipts for keys, and any customer correspondence. These records should be retained and controlled in accordance with **5.7**.

6.2 Initial site inspections

Prior to commencement of a service, the organization should undertake an initial site inspection. A report should be made, identifying any health and safety and security risks that security officers could face in carrying out the service, and presenting information useful for production of assignment instructions.

A competent person should conduct initial site inspections and records should be maintained to confirm that all relevant aspects have been considered. If possible, the report should form part of the proposal to the customer; however, it should be made clear that it is not intended to be a full assessment and recommendation for the overall security of a site.

If the customer declines to have initial site inspections conducted, a letter should be obtained, or notes from a meeting with the customer should be produced, confirming this. In these cases, an assessment should be made by the organization to ensure that health and safety requirements are complied with.

Where existing assignments are taken over, the organization should discuss with the customer and the previous service provider any implications with respect to current employment legislation.

6.3 Assignment instructions

6.3.1 General

Assignment instructions for all duties and responsibilities should be formulated in consultation with the customer and should be available at the start of the contract.

They should clearly show the starting and review dates. Formal reviews of the assignment instructions should be carried out by the organization in consultation with the customer at regular intervals not exceeding 12 months and this should also include a review of the customers site/s health, safety and security risk assessment/s.

Assignment instructions should be agreed, and copies signed by the organization and customer.

If the customer is reluctant to sign the assignment instructions, a copy should be sent to the customer with a letter stating that, in the absence of indication to the contrary, those assignment instructions apply.

Security officers should be familiar with the assignments on which they are working, and should sign to confirm they have read and understood the assignment instructions.

6.3.2 Content

The following details should be included in the assignment instructions:

a) the location, description and extent of the site or property;

b) the agreed means of access;

c) emergency procedures and lines of communication;

d) frequency and method of communication with the control room, including the frequency of check calls;

e) availability of customer's facilities, vehicles or equipment for use by security officers;

f) accountability for and restrictions on a security officer's actions;

g) information on hazards, as identified during the initial site inspection (see **6.2**);

NOTE Attention is drawn to the requirements of the Health and Safety at Work etc. Act 1974 [6] regarding the provision of information on hazards.

h) the number of personnel involved in the assignment, and their individual duties and responsibilities, including:

1) working hours and any hand over requirements;

2) any patrol routes, and routine reporting points and times;

3) the management of CCTV surveillance systems and/or other specifically requested services;

4) access control and searching procedures;

5) record keeping.

6.3.3 Amendments

Any permanent alteration to the instructions that results in changes to security officers' duties or operational requirements should be agreed between the organization and the customer in writing.

Minor amendments should be approved by the organization, and details sent to the customer.

Assignment instructions should be amended and reissued as soon as practicable after changes have been agreed.

Temporary alterations should be recorded in the site records (see **6.4.3**).

6.4 Static sites

6.4.1 Information

Security officers should be familiar with their general and specific site duties and responsibilities.

These should be fully documented in the form of assignment instructions (see **6.3**) and be available to each security officer at their normal place of work.

6.4.2 Duties

The prime responsibility of a security officer should be to protect the customer's people, property and assets at all times, as far as they can reasonably do so.

Typical duties could include, but are not limited to:

a) regular tests of timing, communication, safety or other equipment specified in the assignment instructions;

b) regularly checking that the site has been secured;

c) the management and/or monitoring of movement of people, goods or transport;

d) undertaking site patrols to inspect for breaches in security or other specified changes;

e) making check calls and/or receiving and handling external calls and enquiries;

f) managing the movement of keys and/or other items of equipment for which the organization is responsible;

g) managing and reporting incidents and emergencies.

NOTE Attention is drawn to the Working Time Regulation 2003 [2]

6.4.3 Site records

A daily register should be maintained of all assignments. All occurrences, incidents and actions taken should be recorded, by time and date, in the register. These records should include:

a) the signing-on and -off of the organization's employees (including supervisory visits);

b) changes in the assignment instructions;

*NOTE The customer should approve any such changes (see **6.3.3**).*

c) the times of check calls;

d) the movement of keys or other items of equipment for which the organization is responsible;

e) records of incidents, which should include the following:

1) the date, time and place of the incident;

2) nature of the incident (i.e. fire, flood or theft);

3) the date and time of reporting, and the name of the reportee;

4) details of the incident;

5) action taken, including onward reporting;

6) action to be taken;

7) name(s) and address(es) of person(s) who witnessed the incident.

If there is a separate incident report system in use, either on the customer's site or within the organization, then only items 1) to 3) and the reference number of the incident report needs to be recorded.

6.4.4 Static site performance monitoring

Each static site should have a written plan for regular supervisory/management visits. A qualified person who is independent of the running of that static site should undertake the visits that should include checks on:

a) the validity of the assignment instructions;

b) the satisfactory maintenance of records.

*NOTE 1 The visit might also include items as detailed in **6.4.5**.*

There should be clearly defined procedures for management follow-up to incidents, and for response and support to security officers if incidents occur.

If the security officer does not contact the control room on time, as specified in the assignment instructions, the supervisor should be notified and a visit to the static site should be made or the relevant escalation procedure implemented.

A formal minuted meeting should take place with the customer to discuss contract performance against both the contract and the assignment instructions.

NOTE 2 Additional information such as Key Performance Indicators (KPI) and Service Level Agreements (SLA) could aid the review process.

The frequency of the meetings should be documented and subject to agreement by both parties. Copies of the minutes should be retained on the customer file.

Records of monitoring should be available for inspection by the customer. Where static sites are monitored by mechanical or electronic clocking systems, records of transactions should be made available for inspection by the customer upon request.

6.4.5 Staff visits

Security officer's should receive a welfare check at least once a month from either the static site based supervisor/manager or a supervisor/manager from the organization.

NOTE The monthly welfare check can be conducted by either phone or site visit.

A note of the monthly welfare check should be entered onto a log sheet recording date and time and retained on the security officer's file.

Each security officer should receive a visit at least once every 3 months from either the static site based supervisor/manager or a supervisor/manager from the organization.

The welfare of the security officer should be discussed monthly. The following items should be discussed monthly if necessary, i.e. if there have been changes to the security officers duties or circumstances, as well as during the 3 monthly site visit regardless of any changes:

a) familiarity with assignment instructions and service delivery;

b) performance;

c) training needs.

A supervisor/manager visit report should be recorded electronically or a visit report form should be completed, signed by the security officer and retained on the security officer's file.

Organizations should have processes in place to ensure that security officer's can raise issues outside of the monthly welfare contact or visits.

Annually, a performance appraisal visit should be carried out, the appraisal form should be recorded electronically or signed by the officer and retained on the security officer's file.

Performance appraisals should:

1) be carried out by supervisors/managers with appropriate skills and training in appraisal and people development;

2) be a two-way, confidential and private discussion between supervisor/manager and security officer;

3) focus on past performance (to confirm actions completed and recognize improvements), as well as future needs to improve performance;

4) ideally include both positive and negative feedback from other security officers and customers;

5) identify relevant objectives (e.g. KPI s, personal development objectives) with achievable targets;

6) encourage self-learning and development;

7) encourage those with potential to access opportunities to progress within the organization and to identify and encourage future leaders;

8) be scheduled to take place at an agreed time, ideally away from the normal place of duty and when operational activities can be temporarily covered by another security officer.

6.5 Mobile patrol services

6.5.1 Requirements

Security officers whilst on a mobile patrol should have access to assignment instructions for each site to be visited. The assignment instructions should detail their general and specific site duties and responsibilities.

Assignment instructions should not include customer contact details.

Assignment instructions should be held separately from any related keys, and their relationship should not be ascertainable by unauthorized persons.

Mobile patrol visits should be verified by documented or mechanical/electronic systems and be available for inspection by the customer.

6.5.2 Duties

The prime responsibility of a security officer on mobile patrol should be to make prearranged visits to inspect the sites as detailed in the assignment instructions and to ensure that they are secured as far as reasonably possible.

At the start of duty, security officers should sign for keys in the key register (see **5.2.7**), and sign again, next to the corresponding first entry, when returning the keys at the end of duties.

Where automated patrol systems are not used security officer's should make check calls to the control centre on arrival and departure from site giving their location and details of the next site to be visited. Additional check calls should be made to ensure that the frequency between calls is no more than 1 hour.

NOTE It might be necessary to consider conducting mobile patrols at random times and varying the route to and from the sites to ensure that no patterns can be established.

6.6 Control of keys

6.6.1 General

Organizations providing the management of keyholding and response services should do so in accordance with BS 7984.

The security of keys held or managed by the organization should be controlled in a manner that prevents misuse.

A receipt should be given for keys that are provided by the customer solely for the use of the organization.

Receipts should detail the date and time of the exchange and the person receiving the keys, together with a description of the keys. Receipts should be signed and a copy provided to the customer.

Where keys are managed by the organization, but are not solely for its use, a register describing the keys and their status and location should be maintained.

If keys held by the organization are unclaimed on cessation of a contract, their period of retention and method of disposal (see **6.1.4**) should be recorded and the record retained for seven years.

6.6.2 Keys on static sites

When not in use, keys should be kept in a secure manner.

Each set of keys should be stored ready for inspection at all times and should be uniquely referenced with its details recorded in a key register.

The movement of keys should be traceable. A record should be maintained in the key register of:

a) the location of the keys at all times;

b) the name of the person who has possession of the keys;

c) the date and time of the keys' issue and return.

Keys should be monitored for their safe return. If keys are expected to be on issue for longer than normal, a record should be made of their expected return time. If a key is not returned within the expected period, action should be taken as specified in the assignment instructions.

Supervisory staff or management should check and confirm every 3 months that all stored keys match the key register.

A procedure should be implemented to effect formal hand over of key control between shifts.

6.6.3 Keys on mobile patrols

When not in use, keys should be kept securely within a control room or secure facility located within the premises owned or leased by the organization (to which access is restricted to the organization's employees). If the secure facility is left unattended, it should be protected by a remote-signalling intruder alarm conforming to BS EN 50131-1/PD 6662. If the secure facility is within a vehicle, the vehicle should be protected as described in **5.4.2**.

Each set of keys should be controlled and stored ready for inspection at all times. The set of keys should be uniquely numbered and the number recorded in a key register (see **5.2.7**). Keys should be coded in a manner that does not indicate directly the name and address of the site to which they belong.

Addresses relating to the key codes should be recorded in the key register. When not in use, the key register should be kept within a secure facility in another area. At least weekly, the organization's management should ensure that the stored keys match the key register and that all movements have been properly recorded. Where keys are held which are not in regular use (i.e. daily or weekly), these should be kept in a manner which would indicate any use, such as a separate key cabinet which is additionally secured with a security seal.

NOTE During the weekly check, the management would only need to check the security seal and not each individual key, unless the seal has been broken.

At least every 3 months, the management should confirm that all stored keys match the key register.The organization should confirm and record that this procedure has been carried out.

Keys should be kept in a secure manner or within a vehicle safe.

Keys fixed to a carrying device should remain in the possession of the security officer during the mobile patrol duty period.

If the keys are kept in a vehicle safe (see **5.4.2.2**) the vehicle should be locked when not occupied.

When the vehicle is not operational, keys should not be kept within it.

At the end of each patrol, keys that have been issued should be returned and inspected to ensure that the keys remain securely affixed. All key movements in and out of storage should be recorded in the key register.

Annex A (informative)

Use of the term "security guarding"

The term "security guarding" used in the scope of this standard applies to activities which are described as follows in the Private Security Industry Act 2001 [4]:

a) guarding premises against unauthorized access or occupation, against outbreaks of disorder or against damage;

b) guarding property against destruction or damage, against being stolen or against being otherwise dishonestly taken or obtained.

References to guarding premises against unauthorized access include references to being wholly or partly responsible for determining the suitability for admission to the premises of persons applying for admission.

References to guarding against something happening include references to so providing a physical presence, or carrying out any form of patrol or surveillance, as to deter or otherwise discourage it from happening; or to provide information, if it happens, about what has happened.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7799-1:2005, *Information technology – Code of practice for information security management*

BS 7872:2011, *Manned security services – Cash and valuables in transit services (collection and delivery) – Code of practice*

BS 7960:2005, *Door supervisors/stewards – Code of practice*

BS 8406:2009, *Event stewarding and crowd safety services – Code of practice*

BS ISO 10002, *Quality management – Customer satisfaction – Guidelines for complaints handling in organizations*

BS ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

PD 5454:2012, *Guide for the storage and exhibition of archival documents*

pr EN 50518-1*, Monitoring and alarm receiving centre – Location and construction requirements*

pr EN 50518-2, *Monitoring and alarm receiving centre – Technical requirements*

pr EN 50518-3, *Monitoring and alarm receiving centre – Procedures and requirements for operation*

Other documents

[1] GREAT BRITAIN. Rehabilitation of Offenders Act, 1974. London: The Stationery Office.

[2] GREAT BRITIAN. The Working Time Regulation 2003. London: The Stationery Office.

[3] GREAT BITAIN. The Equality Act, 2010. London: The Stationery Office.

[4] GREAT BRITAIN. Private Security Industry Act 2001. London: The Stationery Office.

[5] GREAT BRITAIN. Data Protection Act, 1998. London: The Stationery Office.

[6] GREAT BRITAIN. Health and Safety at Work etc. Act 1974. London: The Stationery Office.

Websites

http://sia.homeoffice.gov.uk [last viewed 29 August 2013]

http://www.hmrc.gov.uk/leaflets/labour-providers-due-diligence.pdf [last viewed 29 August]

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.