BS 7984-1:2016

BSI Standards Publication

Keyholding and response services

Part 1: General recommendations for keyholding and response services

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2016

ISBN 978 0 580 90401 1

ICS 13.310

The following BSI references relate to the work on this document:
Committee reference GW/3
Draft for comment 15/30324695 DC

Publication history

First published September 2001
Second edition September 2008
Third (present) edition April 2016

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 20, an inside back cover and a back cover.

Foreword

Publishing information

This part of BS 7984 is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 April 2016. It was prepared by Technical Committee GW/3, *Private security management and services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This part of BS 7984 supersedes BS 7984:2008, which is withdrawn.

Information about this document

This is a full revision of the standard and introduces the following principal changes:

- the text has been modified to take account of the creation of BS 7984-2;
- the standard has been harmonized, where possible, with other service standards such as BS 7984-2, BS 7958 and BS 7499;
- greater flexibility is provided as to how an organization operates in this security sector, i.e. two distinct methods of secure facility and the recommendations for a response centre if provided by the organization (could be a contracted service by another provider); and
- keyholder response officer training has been aligned to the recently published NOSs (National Occupational Standards) in this sector.

Attention is drawn to the Private Security Industry Act 2001 [1], which contains provisions for regulating the private security industry, including security guarding and keyholding. A person falling within the definition of providing security industry services under the Private Security Industry Act 2001 [1] is required to be licensed in accordance with that Act.

Use of this document

As a code of practice, this part of BS 7984 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 part of BS 7984 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 part of BS 7984 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.

This page deliberately left blank

Introduction

This British Standard gives recommendations for keyholding and response services. It details the manner in which an organization manages the service provision of keyholding and how it should respond to an event. In addition to key management, it further details what is expected of a response centre and vehicles used for the storage of keys.

Elements of keyholding are also contained in BS 7499; however, BS 7499:2013, **5.4.2.2** clearly states that where an operational vehicle is required for keyholding and alarm response, the response is to be carried out in accordance with BS 7984.

NOTE BS 7984-2 covers response services provided by lone workers.

This British Standard is intended to be used in conjunction with the National Occupational Standards for responding to keyholding attendance requests and covers the following activities:

a) response to keyholding attendance requests;

b) attendance at sites in response to keyholding attendance requests;

c) locating causes of security and safety alarms;

d) making premises secure and complete keyholding attendance;

e) preserving potential evidence of security breaches;

f) dealing with conflict when making keyholding attendances; and

g) carrying out site inspections to support keyholding activities.

Although this British Standard is aimed at organizations that provide keyholding and response services on a contracted basis, its provisions and guidelines could be equally applicable to those companies operating an in-house service provision.

1 Scope

This British Standard gives recommendations for the management, staffing and operation of an organization providing keyholding and response services or keyholding response services and mobile patrols as a shared service on a contracted basis.

This British Standard does not apply to lone worker response services, static site guarding and mobile patrol services.

NOTE Recommendations for lone worker response services are given in BS 7984-2. Recommendations for static site guarding and mobile patrol services are given in BS 7499.

This British Standard assists procurers of keyholding and response services such as security companies and agencies, building management companies, local authorities and those promoting compliance.

2 Normative references

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

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

PD 6662:2010, *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 specific contractual duties

NOTE The document can be either a hard copy or an electronic copy.

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

3.3 controller
person designated to manage, control and report on keyholding and response services

3.4 customer
individual or body retaining the services of the organization

3.5 event
incident requiring entry or attendance at a customer's location as determined by contractual requirements

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

NOTE 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.

3.7 keyholding response
service whereby the organization holding keys to a customer's premises attends in response to a request

3.8 keyholding response officer
trained person who attends a location (as determined by contractual requirements) in response to an event and, when required, provides guarding services

NOTE Attention is drawn to the Private Security Industry Act 2001 [1] and the need for private contractors to hold the appropriate licence to undertake designated activities.

3.9 key(s)
physical instrument or data allowing authorized access to a customer's premises

3.10 organization
sole or main provider of keyholding and response 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 response centre
secure location from which a controller operates

3.13 secure facility
place in which keys and/or assignment instructions are stored and from which they are provided in responding to an event

*NOTE See **5.2** for further information.*

3.14 subcontract
all, or part, of a contract assigned to another service provider, where the subcontracted services provider is responsible for service delivery including the supply and management of their employees in fulfilment of the subcontract

3.15 subcontracted service
provision of services on behalf of a principal contractor

3.16 subcontracted services provider
self-employed individual or a company that is contracted to provide service delivery on behalf of the principal contractor

NOTE The principal contractor is ultimately responsible and accountable for service delivery to the customer.

3.17 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

4 The organization and documented information

4.1 Structure

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

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 or director should be disclosed on request.

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

NOTE 2 Attention is drawn to the Data Protection Act 1998 [3] and the rights of an individual regarding access to information about their convictions and cautions.

The organization should operate a documented complaints management system.

NOTE 3 Guidance is given in BS ISO 10002.

4.2 Finances

The organization should be able to present two years' annual trading accounts, certified by an accountant, 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.

The organization should prepare annual accounts in accordance with applicable accounting standards. The accounts should be certified by an accountant 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, including public liability, employer's liability, efficacy, loss of keys, consequential loss of keys, fidelity guarantee, professional indemnity, wrongful arrest and vehicle insurance.

NOTE The following insurance cover could also be considered: legal expenses, directors' and officers' liability.

4.4 Documented information

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 **6.1.2**).

NOTE 1 Attention is drawn to the Data Protection Act 1998 [3].

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 ISO/IEC 27002. Guidance 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) key registers and incident reports;

c) details of persons deployed to the assignment;

d) training records;

e) rosters; and

f) risk assessments.

An employee's basic records (as detailed in BS 7858) should be kept for at least seven years after 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.

4.5 Subcontracted services

The organization should obtain the customer's agreement regarding conditions for the use of subcontracted service providers for undertaking the duties of keyholding response officers and controllers.

The subcontracted services provider should also follow the recommendations given in this British Standard. The organization should satisfy itself that these recommendations have been followed. There should be documented evidence that due diligence has been carried out.

5 Premises

5.1 General

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

5.2 Secure facility

A secure facility should be one of the following.

a) A soundly constructed building, protected by a remotely monitored intruder alarm conforming to PD 6662:2010, grade 3, containing a dedicated room or lockable cabinets provided for the storage of keys; cabinets should be securely fixed to the fabric of the building. Where there is a shared occupancy, the intruder alarm system for the secure facility should be under the sole control of the organization.

b) A vehicle fitted with an alarm, an immobilizer, containing a lockable means of storing keys, which should be securely fixed to the body of the vehicle being used for the storage of keys.

5.3 Response centre

5.3.1 General

Where the organization operates a response centre, it should perform the following functions:

a) provision or procurement of assistance, information or advice for keyholding response officers in routine and emergency situations, including any form of follow-up action as a result of a missed check call;

b) effective monitoring of keyholding response officers and mobile supervisory staff by observance of documented, established routine telephone, radio or other communication procedures;

c) recording, in accordance with **5.3.3**, all appropriate routine and emergency matters; and

d) recording movement of the customer's keys held by the organization.

The response centre should be housed within a secure facility, and be a restricted area, accessible only to authorized personnel. Visitors should be accompanied at all times by an authorized person.

NOTE Authorized personnel are to be defined by senior management.

5.3.2 Operations

Procedural instructions should be provided for guidance of response centre staff. The instructions should enable response centre staff to deal effectively with routine matters and emergencies. The instructions should clearly indicate stages at which an event should be escalated to more senior personnel. The instructions should be readily available within the response centre at all times.

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

Response centre staff should have immediate access to the following:

a) full assignment instructions for all contracts;

b) names, addresses and telephone numbers of all operational staff, including supervisors and management;

c) emergency contact records for all customers;

d) telephone numbers of police stations within the operational area of the response centre;

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

f) emergency procedures and contingency plans in case of fire, flood or bomb threat.

5.3.3 Records

The following records should be kept.

a) Records of events, for a minimum of 12 months from the date of the event. Entries should be uniquely referenced and should include the date and time of the event, and the name of the controller completing the record.

b) Records of radio and telephone calls from keyholding response officers for a minimum of 12 months.

c) Details of check calls, with missed and late check calls shown.

Precise times of contact should be included.

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

6 Personnel

6.1 Employees

6.1.1 General

The organization should ensure that it has employed sufficient keyholding response officers to fulfil its contractual obligations and sufficient supervisory personnel to manage those contracts.

6.1.2 Selection and screening

All persons undertaking, or having access to details of an assignment, keyholding and response 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.

All persons should also be able to demonstrate satisfactory reading, writing and verbal communication abilities.

Only persons of competence and integrity should be employed and a personal interview should be conducted to assess suitability.

Full pre-employment enquiries should be carried out to confirm an applicant's identity and to ensure that they are suitably qualified.

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

NOTE 1 Attention is drawn to the Working Time Regulations 1998 [4], part 2 section 7.

Employers should validate the employee's driving licence against company policy for those employees whose duties involve driving. The employer should check the employee's driving licence and carry out a DVLA licence check on the employee every six months. Records should be maintained and retained.

NOTE 2 The employer may use an automated system to receive authorized notifications of licence changes via the DVLA.

6.1.3 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, as there might be medical considerations which could fundamentally inhibit the employee from carrying out the job.

NOTE 2 Attention is drawn to the Equality Act 2010 [5].

In order to ensure that the physical condition of keyholding response 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 risks 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.

6.1.4 Terms and conditions of employment

Employees should receive a written statement of the terms and conditions of their employment, which should include details of the following:

a) job title;

b) job description;

c) effective start date;

d) probationary period, if required;

e) provisional period subject to screening, if applicable;

f) pay and allowances;

g) hours and days of work;

h) leave entitlement;

i) conditions of payment during absence through illness;

j) pension entitlement;

k) industrial injury procedures;

l) the address of the organization;

m) equipment and uniform supplied;

n) disciplinary and appeals procedures; and

o) terms of notice of termination of employment.

Persons 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 the Working Time Regulations [4].

6.1.5 Disciplinary code

Employees should be instructed that the following (including the aiding and abetting of others) 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 those substances 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; or

   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, see the SIA website for details. [1)]

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

[1)] <http://www.sia.homeoffice.gov.uk> [last viewed 25 April 2016].

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

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 that might also constitute criminal offences.

6.1.6 Identification

Employees, who are required to be screened in accordance with **6.1.2**, 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); and

d) a current photograph of the employee.

Employees should be required to carry their identity cards while 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 keyholding response officer is required to display a SIA licence this does not negate the need for company identification.

6.2 Equipment and uniforms

6.2.1 Uniform

Unless otherwise requested by the customer, employees should wear the uniform supplied when on duty.

Employee uniforms should clearly display the insignia of the organization.

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

6.2.2 Vehicles

Operational vehicles should:

a) be appropriate for the intended use;

b) carry a two-way communication device;

c) allow for the organization to ascertain the destination or location of the vehicle at all times, for example, through the fitting of a tracking device, or a GPS signal;

d) be inspected by the driver at the start of each shift to ensure that it is appropriate for the intended use;

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

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

g) have any damage repaired as soon as possible;

h) be kept clean and tidy; and

i) not carry any passengers not on official duty.

NOTE Unless they are involved in covert operations or otherwise excepted from doing so under contract, it is desirable for operational vehicles to clearly display the organization's name, badge or logo, and telephone number.

Vehicles being used as a secure facility should conform to **5.2**b).

6.2.3 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.

6.2.4 Equipment records

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

Records of equipment repaired should be kept and maintained for at least 12 months or longer, if the records are required for the investigation of an incident.

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.

6.3 Training

6.3.1 General

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

6.3.2 Induction training

The organization should provide induction training in matters related to conditions of employment and organizational procedures for all employees; this induction training is additional to the basic job training described in **6.3.3**. Induction training should be completed before the keyholding response officer is deployed on operational duties.

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

6.3.3 Basic job training

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

NOTE 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 [1] 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 sector-competent, qualified training persons, in a room that is adequately equipped and conducive to effective learning. Training should last at least 32 hours, including examination, and should cover the following core subjects:

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

b) patrolling;

c) control of access and egress;

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; and

m) communication skills and conflict management.

When the training period is complete, the trainee should take a written examination comparable with a national recognized qualification which meets 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 licence (including those who have transitioned from a door supervisor licence to security guarding) or close protection licence who wish to work in the security guarding area. Any training identified by the gap analysis should be provided.

6.3.4 Keyholding and response officer training

Training should be provided by sector competent, qualified training persons in a room that is adequately equipped and conducive to effective learning.

Training should last a total of at least 16 hours in addition to the basic job training (see **6.3.3**), including an examination, and should cover the following performance criteria competencies as defined by the SSB:

a) collate and confirm information about attendance requests;

b) prioritize keyholding response attendances and other actions;

c) allocate resources for keyholding response;

d) take responsibility for keys and site information and equipment;

e) travel between sites safely and efficiently;

f) carry out dynamic risk assessments on arrival;

g) enter sites and premises;

h) maintain the security of premises whilst locating sources of alarms;

i) determine causes of alarm activations;

j) confirm physical security of premises and set security systems;

k) complete keyholding attendances;

l) preserve the integrity of potential evidence;

m) record and report details of potential evidence;

n) recognize potential conflict situations;

o) respond to conflict situations;

p) inspect sites to collect information to support keyholding activities;

q) produce keyholding site inspection reports and assignment instructions; and

r) maintain records, keys and equipment to support keyholding activities.

During the first three months of employment, the competence of the response officer should be assessed by a suitably qualified or experienced supervisor or manager.

6.3.5 Response centre training

Training and instruction of response centre personnel should include the following:

a) outline of response centre operations;

b) detailed explanation of duties;

c) radio and telephone procedures;

d) documentation and recording procedures;

e) emergency procedures;

f) location and use of response centre records;

g) explanation of keyholding response officers' rosters;

h) explanation of response centre personnel rosters;

i) collation and provision of information about response events; and

j) allocation of resources for keyholding response.

6.3.6 Takeovers

If employees are acquired through a takeover, the organization should identify their training needs and address them in line with the recommendations in this British Standard.

6.3.7 Refresher training

The effectiveness of all employees should be continuously monitored. If the effectiveness of an employee is found to be unsatisfactory, refresher training should be provided by suitably qualified persons as soon as practicable.

6.3.8 Contingency training

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

6.3.9 Training records

All training provided and qualifications achieved should be accurately recorded on a form specific for the purpose, be signed by the trainee, countersigned by the trainer and retained. If a certificate of competence is provided by a recognized and relative sector competent training organization, a copy should be retained. Where records are held directly by the organization, they should be retained for a period of seven years.

NOTE Attention is drawn to the Skills Funding Agency's Learning Records Service (LRS). Organizations can complete a Personal Learning Record for each employee, which stores all the employee's learning achievements. Details of courses recently completed (starting from the 2007/08 academic year) or currently in progress with a recognized learner are automatically added to the register. This includes courses from school and further education, but not higher education. The student can also add course details themselves. Information about the purpose of LRS can be found at www.gov.uk/government/collections/learning-records-service.

7 Service provision

7.1 Sale of services

7.1.1 Contacting prospective customers

When contacting potential customers in order to promote keyholding and response 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.

7.1.2 Customer information

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

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

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

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

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

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

4) 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 the keyholding response officers;

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) type and extent of insurance cover;

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

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

7.1.3 Quotations

A clear written quotation should be provided by the organization. If the quotation is accepted by the customer, it should form part of the contract (see **7.2**). 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 **7.3**) 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 the expected response to events (including response times), provision of specialist advice or duties (e.g. areas specifically to be inspected and any limitations) 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 contract;

l) the obligation of the customer to satisfy themselves that if an external key storage facility at the customer premises (see **8.5**) is to be used that this method of storage is acceptable to their insurers;

m) the means for reporting and exchanging operational information, including specified contingency plans;

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

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

p) that keyholding and response services can be provided simultaneously for a number of customers, and that, accordingly, interruptions or delays can occur if an event occurs at the premises of another customer during the course of a keyholding response officer's duties.

7.2 Contracts

7.2.1 General

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.

7.2.2 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 **4.4**.

7.3 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 keyholding response officers could face in carrying out the service, and providing information useful for production of assignment instructions.

NOTE Attention is drawn to the requirements of the Health and Safety at Work Act 1974 [6].

A competent person should conduct initial site inspections, and records should be maintained to confirm that all relevant aspects have been taken into account. 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 the 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.

7.4 Assignment instructions

Assignment instructions for all duties associated with keyholding and response services should be agreed and approved by the organization and customer, and should be available at the start of the contract.

Assignment instructions should be updated on notification of changes by the customer, and any amendments recorded. Temporary alterations to the instructions should be recorded in the assignment documentation.

Assignment instructions and emergency and site information should be readily available to personnel on duty. Assignment instructions issued to keyholding response officers should not include the premises' address or other means of site identification.

Assignment instructions should include, though not be limited to, details of the following:

a) hazardous conditions (health and safety assessments);

b) agreed means of access;

c) method of operating/re-setting alarm;

d) client specific instructions;

e) location of main services; and

f) contingency plans.

7.5 Keyholding and response to events

7.5.1 General

The organization should respond in accordance with the contract they have with the customer.

The date and time of notification of an event should be recorded, and from whom it was received. There should also be a record of the responding officer.

7.5.2 Keyholding response officers

Keyholding response officers should have access to up-to-date assignment instructions when responding to an event.

Keyholding response officers should make check calls on arrival and departure, giving their location and, where applicable, details of the next premises or location to be visited. In all circumstances a check call should be made at least once per hour. Where electronic check calls are made they should be made by a secure method that identifies the individual.

Upon completion of an event a record should be made by either the keyholding response officer, or the response centre, as appropriate, and should include the following:

a) location of the event;

b) date and time of arrival at and departure from the event;

c) details of the event;

d) action taken;

e) names and contact details of persons present at the event; and

f) authorization from the client and/or organization to depart.

The keyholding response officer should not leave the location of the event until authorized.

7.5.3 Follow-up

Procedures should be in place setting out how the organization follows up on events as agreed with the client.

8 Key management

8.1 General

Procedures should be in place to ensure the security and disposal of the keys, and that records are maintained (see **5.3.3**).

An effective management audit system should be in place to verify that the recommendations of this British Standard have been followed.

8.2 Initial receipt of keys

A receipt should be made out for the key provided by a customer for keyholding services. 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.

Keys should be deposited within a secure facility (see **5.2**) without delay and details recorded in the key register.

8.3 Control of keys

*COMMENTARY ON **8.3***

*This subclause refers to control of physical keys. For guidance on control of data, see **4.4**.*

Within the secure facility each set of keys should be securely controlled to prevent unauthorized access in a manner that prevents misuse. Keys should be kept sealed; the seal should be uniquely numbered and non-reusable and the number recorded in the key register. Access to new seals should be restricted to authorized personnel.

A key management log should be maintained and stored securely, recording date, time and reason for use (see **5.3.3**).

When not in use, keys should be kept within a secure facility. If the secure facility is within a vehicle, the vehicle should be protected as described in **5.2**b).

Each set of keys should be stored ready for inspection at all times. The set of keys should be uniquely numbered and the number recorded in a key register [see **4.4**b)]. Keys should be coded in a manner that does not indicate directly the name and address of the site to which they belong.

At least quarterly, the management should confirm that all stored keys match the key register.

At the end of each event, 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.

8.4 Returning and disposal of keys

The organization should surrender any of the customers' keys to the customer when requested to do so, in writing, or upon termination of the contract.

Keys should be returned in one of the following ways:

a) to the customer's representative calling at the organization's office by prior appointment;

b) by a postal or courier service providing for signed and dated delivery, collection and full tracking of consigned packages; or

c) by special arrangements set up by the customer in conjunction with senior management of the organization.

If keys are unclaimed on cessation of a contract, they should be securely disposed of after one month and a record of the method of disposal retained for seven years.

8.5 Key storage at customer facilities

*NOTE The use of a customer's key storage facility at the premises by means of external boxes or vaults might not be as secure as the methods described in **5.2** and might be in breach of an interested insurer's policy terms and conditions, for example an intruder alarm condition requiring that customers remove all alarm operating devices (e.g. unsetting fobs/transmitters) from a premises when they are left unattended.*

Organizations carrying out keyholding and response services should request a specific written acknowledgement and acceptance from the customer of any potential security risks relating to keys and/or electronic security systems (e.g. intruder alarms or CCTV) from the use of external boxes or vaults, and should also recommend that the customer consults their insurer(s) before signing it.

If the customer is reluctant to provide a written acknowledgement, the organization should retain evidence that they have made the customer aware of the potential security risks.

Keys held in an external box or vault are not deemed to be under the organization's control, and the provisions of **8.1** to **8.4** should not be applied to their management and control.

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 7499, *Static site guarding and mobile patrol service – Code of practice*

BS 7984-2, *Keyholding and response services – Part 2: Lone worker response services*

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

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

BS ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

PD 5454, *Guidance for the storage and exhibition of archival documents*

Other publications

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

[2] GREAT BRITAIN. Rehabilitation of Offenders Act 1974. London: HMSO.

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

[4] GREAT BRITAIN. Working Time Regulations 1998. London: The Stationery Office.

[5] GREAT BRITAIN. Equality Act 2010. London: The Stationery Office.

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

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.