



National Security Inspectorate

Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY

E: nsi@nsi.org.uk | W: nsi.org.uk

Security.Improved

Date: 07 July 2020

To: All NSI Guarding Gold and Guarding Silver approved companies and applicants

TECHNICAL BULLETIN No: 0051

Publication of BS 7499:2020 – Code of practice for the provision of static guarding security services

BS 7499:2020 was published on the 30th April 2020 and is available from the BSI or NSI as an individual purchase or through the NSI Standards on Subscription service for approved companies.

Implementation timescale for applicant companies

New applicant companies will be audited against BS 7499:2020 with immediate effect and any Improvement Needs recorded against clauses of the Standard will have to be satisfactorily addressed before approval can be granted.

Where an application for approval was already in progress with the NSI before the date of this Technical Bulletin, then the approval will continue to progress against the appropriate standards.

Implementation timescale for existing approved companies

Existing NSI approved companies will be required by NSI to be compliant with BS 7499:2020 by the 31st March 2021.

Where the actual wording of the Standard is quoted, it is reproduced in bold text.

Where it is considered relevant, further clarification is included in italics.

Please note this is not a definitive list of all the changes introduced through the publication of the revised 2020 edition of BS 7499. Only significant changes are detailed within this document.

BS 7499:2020 references BS 10800:2020 which is an overarching standard and which will become applicable to all security service sectors, e.g. security guarding, mobile patrol, key-holding, door supervision, close protection, cash in transit, security dogs, events security, CCTV management and operation, provision of lone workers. etc. when they become due for review and a new edition is published.

BS 10800:2020 now contains all requirements that are common to the sector specific British Standards, for example Structure, finance insurance etc .

The recent publication of BS 7499:2020 and BS 7984-3 are the first standards to reflect this change.

The requirements relating to mobile patrol services have been removed from the latest edition of BS 7499 and are now to be found in a new standard BS 7984-3:2020 to align with the BS 7984 series.

Scope

This British Standard gives recommendations for the management, staffing and operation of an organization providing security guarding services on a static site.

NOTE Annex A gives information on the use of the term “security guarding”.

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

NOTE Recommendations for cash-in-transit services, CCTV, door supervisors, keyholding and response services, mobile patrol services and event stewarding are given in BS 7872, BS 7958, BS 7960, BS 7984-1, BS 7984-3 and BS 8406 respectively.

The scope no longer covers mobile patrols but does include a reference in the second note to the new standard BS 7984-3 - Provision of mobile security services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document.1) For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7858, Screening of individuals working in a secure environment – Code of practice

BS 10800:2020, Provision of security services – Code of practice

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

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

References to BS 7984, BS 7858, BS 5979 and BS 5839 are no longer applicable.

3 Terms and definitions

The terms ‘principal’ and ‘supplier’ are no longer defined.

3.7 customer property

asset in which a customer has a legal financial interest

This is a new definition.

3.10 key register

documented record that allows an organization to confirm the location of keys at all times, the name of the person who has possession of the keys and the date and time of the keys' issue and return

This is a new definition.

3.11 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE The concept of organization includes, but is not limited to: sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

This term has changed to remove reference to mobile patrol.

3.13 security officer

person who performs contractual duties at a site

This term has changed to remove reference to mobile patrol.

3.14 site

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

This term has changed from 'static site' to 'site'.

3.15 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

NOTE When deployed, subcontracted labour remains under the direction and control of the subcontracting company.

This is a new definition.

4 The organization

4.1 Structure

The organization should follow the recommendations given in BS 10800:2020, 8.2.

4.2 Finances

The organization should follow the recommendations given in BS 10800:2020, 7.2.

4.3 Insurance

The organization should follow the recommendations given in BS 10800:2020, 7.3.

NOTE The organization might wish to specifically consider cover for inefficacy/efficacy, fidelity bonding, contractual liability, loss of keys and consequential loss of keys and wrongful arrest (this list is not exhaustive).

4.4 Documented information

The organization should follow the recommendations given in BS 10800:2020, 7.11.

NOTE BS 10800:2020, 7.11 covers creating, updating and maintaining documented information, and also covers records and record keeping.

The Organisation section has an extra sub-clause 'Documented information', all clauses in this section now refer to clauses in BS 10800:2020.

5 Resources

5.1 Premises

The organization should follow the recommendations given in BS 10800:2020, 7.4.

5.2 Control room

5.2.1 Design, construction and layout

The organization should follow the recommendations given in BS 10800:2020, 7.5.

The organization should determine the design, construction, layout and equipment requirements for its control rooms. The requirements should respond to the needs of staff using these facilities (e.g. accessibility). The level of design, construction, layout and equipment should be directly related to risks associated with customer contracts.

Where control rooms are outsourced, the organization should confirm that the control room(s) conform to BS 10800:2020, 7.5 and are fit for purpose.

Sub- clauses for Premises and its construction refer to requirements in BS 10800:2020.

5.2.2 Location within a secure facility

Control rooms should be situated within premises owned or leased by the organization, and to which the organization has access at all times. The control room should be within a soundly constructed building and, if not continuously staffed, should be protected by a remotely monitored intruder alarm conforming to PD 6662 and BS EN 50131-1. Where there is a shared occupancy, the intruder alarm system for the control room should be under the sole control of the organization.

Control rooms must be within a secure (if not continuously manned be protected by a PD 6662 security alarm) and soundly constructed building situated within premises that are under the control of the organisation operating the control room, e.g. leased or owned.

5.2.3 Control room procedures

A control room manual should be provided to control room staff, which gives procedural instructions. The control room manual should enable control room staff to deal effectively with routine matters and emergencies. The manual should clearly indicate the stages at which an incident should be escalated by the controller to more senior staff or to the customer. A copy of the control room manual should be readily available within the control room at all times.

Records of incidents should include (but are not limited to) 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; and**
- f) names and contact details of persons who witnessed the incident.**

NOTE 1 Attention is drawn to the relevant data protection legislation.

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.

Procedures for daily verification that automated systems are working should be detailed in the control room manual and verifications should be documented.

NOTE 2 Attention is drawn to the HSE publication, Working alone: Health and safety guidance on the risks of lone working [1]. Further information about controlling risks can be found on the HSE website at: www.hse.gov.uk/toolbox.

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

This sub-clause heading has changed from 'Procedures' to 'Control room procedures' and the sub-clause text is amended.

5.2.4 Control room 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 operational staff, including supervisors and management;**
- e) emergency contact records (including telephone numbers) for all customers;**
- f) useful telephone numbers (e.g. emergency services, water companies, electricity companies, boarding-up services);**
- g) a copy of the control room manual;**
- h) emergency procedures and contingency plans in case of fire, flood, terrorist attack or bomb threat;**
- i) a register of keys that are held in the control room; and**
- j) duplicate copies of all the information above, separately and securely stored as a backup with retrieval of documented information tested to verify that backup arrangements are functioning.**

NOTE Attention is drawn to the relevant data protection legislation.

This sub-clause title has changed, from 'Information' to 'Control room information'.

Requirements for contingency planning is now more clearly defined.

There is an additional requirement to provide separate and securely stored duplicate copies of the defined control room information.

5.2.5 Control room records

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 sequentially and should include the time and date of the incident and the name of the controller completing the record.**
- b) Records of all communications 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 supervisory visits.

Where keys are held in the control room, controllers should also maintain a register of keys held and should sign for keys on shift changeover.

NOTE 1 Minimum periods for retention of records can be reviewed, if applicable, for particular purposes, especially with regard to potential liabilities for civil action, for example personal injury (three years) or property damage (six years).

NOTE 2 Attention is drawn to the relevant data protection legislation.

The requirement to record communications from security officers and supervisors has been extended to require all forms of communication are recorded.

5.2.6 Control room staff

The number of controllers on duty should be consistent with the expected workload. Controllers should be trained in accordance with 5.5.5.

This is a new requirement.

5.2.7 Escalation procedures

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 site should be made or the relevant escalation procedure implemented.

The frequency of check calls should be determined following a health and safety and security risk assessment, and should take into account the number of security officers on duty. The rationale for the frequency decided should be documented, and regularly reviewed. The rationale for maintaining the status quo or any changes in the frequency should also be documented, and regularly reviewed.

This is a new requirement.

5.3 Security officers

The sub-clause title has changed from 'Staff' in the 2013 edition. The text has changed to remove any reference to mobile patrol.

Sub-clause 'Selection' and 'Screening' in the 2013 edition is now split into two sub-clauses, one for 'Selection' and one for 'Screening'.

5.3.4 Health

The organization should follow the recommendations given in BS 10800:2020, Annex A.

5.3.5 Terms and conditions of employment

The organization should follow the recommendations given in BS 10800:2020, Annex A.

5.3.6 Disciplinary and grievance code

The organization should follow the recommendations given in BS 10800:2020, Annex A.

Sub-clauses covering 'Health', 'Terms and conditions of employment' and 'Disciplinary and grievance code' all refer to Annex A of BS 10800:2020.

5.3.7 Identification

All employees who are required to be screened in accordance with 5.3.3 should be issued with a form of identification incorporating the following information:

- a) the name and contact details of the organization;**
- b) the name of the employee and employee number;**
- c) the expiry date of the form of identification; and**
- d) a current photograph of the employee.**

Employees should be required to carry their form of identification while on duty.

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

A record of forms of identification issued should be maintained. This record should also indicate the status and location of withdrawn forms of identification, 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.

Changes to the text of this sub-clause dealing with 'Identification' removes the requirement for an identity card as the only form of identification other forms of identification are allowed. Requirements for contact details of the organisation and the time before expiry of the identification are not defined.

5.4 Equipment and uniforms

The organization should follow the recommendations given in BS 10800:2020, 7.6.

NOTE BS 10800:2020, 7.6 has four subclauses which cover uniform, vehicles, use of other equipment and record keeping for equipment and uniforms.

This sub-clause now refers to sub-clause 7.6 of BS 10800:2020.

Sub-clauses in the 3013 edition covering vehicles have been removed and are now included in the new BS 7984-3 standard - Keyholding and response services - Provision of mobile security services.

5.5 Training

5.5.1 General

The organization should follow the recommendations given in BS 10800:2020, 7.7.1 and 7.7.3, with regard to counter-terrorism training.

5.5.2 Induction training

The organization should follow the recommendations given in BS 10800:2020, 7.7.2.

Induction training should be additional to applicable SIA licence-linked training. Induction training should be completed before the security officer is appointed to an assignment.

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

The Training sub-clause refers to sub-clauses in BS 10800:2020. Induction training must be in addition to applicable SIA training.

5.5.3 Operational training

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

Training should be provided prior to commencement of operational duties. Training should be provided by competent, qualified training persons. The training environment should be equipped with all the facilities that are needed to enable the training tasks to be carried out.

Training should cover the duties and complexities of the role being performed, and should cover the elements of the following core subjects as applicable:

- a) introduction to the role;**
- 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; and**
- m) assignment-specific client requirements.**

The title in the 2013 edition 'Basic job training' is renamed to 'Operational training'. The text is modified to remove a specified minimum time for training, reference to a recognised qualification body and additional subject specific training.

5.5.4 Assignment-specific training

New officers on a first assignment, or officers transferring between assignments, should be given on-the-job training tailored to the assignment and to the needs of the trainee and the customer.

A newly-appointed security officer should be supernumerary while becoming familiar with the site requirements for a period that reflects the complexity of the assignment (not normally

less than 8 hours). This period should also reflect the site shift pattern, encompassing both day and night shifts if appropriate.

During the first three months of deployment on each assignment, the competence of the security officer should be assessed by a competent person against performance criteria applicable to the site concerned.

Full training records should be maintained.

This sub-clause has a changed structure and a new requirement that all training records must be maintained.

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) escalation procedures;**
- g) location and use of control room records;**
- h) explanation of security officers' rosters; and**
- i) explanation of controllers' rosters.**

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

This sub-clause has a changed structure with new requirements for escalation training to be carried out and the competency of controllers to be assessed as a minimum of once a year.

5.5.6 Supervisory training

Employees who have supervisory responsibilities should be trained to a proficient standard by competent persons. Training should be provided in the following areas (as appropriate):

- a) the role of a supervisor;**
- b) leadership;**

- c) decision making;
- d) problem solving;
- e) communication skills;
- f) conducting a performance review;
- g) time management;
- h) customer service;
- i) knowledge of disciplinary procedures;
- j) use of appropriate documentation; and
- k) knowledge of escalation procedures.

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

This sub-clause has new requirements to include training on disciplinary procedures, use of appropriate documentation and knowledge of the escalation procedures. The requirement in the 2013 edition to provide team behaviour training has been removed, along with the encouragement to improve the knowledge of specific subjects.

5.5.7 Specialist training

Security officers engaged to perform specialist duties (e.g. first aid, banksman, fire-fighting, lift rescue) should be trained to a proficient standard by competent persons. Training should be provided on the use of all applicable equipment. Training records should be maintained.

This sub-clause includes a new requirement to maintain all training records.

5.5.9 Refresher training

All employees should receive refresher and/or development training as applicable for the role they perform on an annual basis. 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 competent persons as soon as practicable.

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

This sub-clause has a modified requirement to carry out refresher training as a minimum of once a year, rather than carry out training when required as the result of monitoring. The text has changed providing an emphasis on following procedure or legislation change to inform training requirements.

5.5.10 Continuous professional development (CPD)

The organization should encourage employees to pursue relevant sector-specific CPD.

NOTE Organizations are advised to consider encouraging the achievement of recognized formal qualifications, in addition to basic job training, in security disciplines, e.g. qualifications based on the appropriate national occupational standards.

This is a new requirement.

Sub-clauses 5.5.11 Contingency training and 5.5.12 Vocational training contained in the 2013 edition are not included in the 2020 edition of BS 7499.

5.5.11 Training records

The organization should follow the recommendations given in BS 10800:2020, 7.7.6.

This sub-clause refers to BS 10800:2020.

6.1.1 General

The organization should follow the recommendations given in BS 10800:2020, 8.3 and 8.7.

NOTE BS 10800:2020, 8.3 has five subclauses which cover contacting potential customers, the type of information that is to be supplied to potential customers, conducting a pre-quotation survey, producing quotations and contracts. BS 10800:2020, 8.7 covers the use of subcontractors and bought-in-labour.

This sub-clause refers to BS 10800:2020.

Sub-clause 6.1.2 Customer information contained in the 2013 edition is not included in the 2020 edition.

6.1.2 Contract records

The organization should follow the recommendations given in BS 10800:2020, 7.11.

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.

NOTE Attention is drawn to the relevant data protection legislation.

This sub-clause refers to BS 10800:2020.

Sub-clauses contained in the 2013 edition '6.1.3 Quotations', '6.1.5 Contracts' and '6.1.6 Contract records' are now included in BS 10800:2020, sub-clause '6.1.4 Quotations for mobile patrol services' contained in the 2013 edition is now included in BS 7984-3.

6.2 Site surveys

The organization should follow the recommendations for pre-quotation surveys given in BS 10800:2020, 8.3.3 and initial site surveys given in BS 10800:2020, 8.4.

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.

NOTE Attention is drawn to the requirements of the Health and Safety at Work Act 1974 [4].

A competent person should conduct initial site surveys 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 or recommendation for the overall security of a site.

If the customer declines to have initial site surveys 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 verify that health and safety and security 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.

This is a new sub-clause referring to BS 10800:2020.

6.3 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 and egress;**
- c) emergency procedures and lines of communication;**
- d) escalation procedures;**

- e) frequency and method of communication with the control room, including the frequency of check calls;
- f) availability of customer's facilities, vehicles or equipment for use by security officers;
- g) the role of a security officer, including accountability for and restrictions on a security officer's actions;
- h) information on hazards, as identified during the initial site survey (see 6.2);

NOTE Attention is drawn to the requirements of the Health and Safety at Work etc. Act 1974 [4] regarding

the provision of information on hazards.

- i) the number of security officers involved in the assignment, their objectives and individual duties and responsibilities, including:

- 1) working hours and any handover 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; and
- 5) record keeping, including reporting.

This sub-clause includes two new requirements to provide assignment instructions that must include escalation procedures and reporting.

6.3.4 Review

Assignment instructions should be reviewed at regular intervals, not exceeding 12 months.

This is a new requirement.

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 of a security officer should 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 and remains secured;

- c) the management and/or monitoring of movement of people, goods, assets 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; and
- g) managing and reporting incidents and emergencies.

NOTE Attention is drawn to the Working Time (Amendment) Regulations 2003 [2].

This sub-clause has a small amendment to requirement b) requiring a need to check the site remains secure.

6.4.3 Site records

Daily registers should be maintained on all assignments. All occurrences, incidents and actions taken should be recorded, by time and date, in the registers. These records should include:

- a) the signing-on, and -off, of the organization's employees (including supervisory visits);
- b) changes in the assignment instructions [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; and
 - 7) name(s) and contact details of person(s) who witnessed the incident.

NOTE 1 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.

f) the details and nature of patrols.

NOTE 2 Attention is drawn to the relevant data protection legislation.

This sub-clause contains amendments to the requirements requiring that changes to assignment instructions must be agreed by the customer, records of actions taken must also include any onward reporting and the contact details of a witness to an incident need not include a full address.

6.4.4 Site visits

The organization should have a written and communicated plan for regular supervisory/management visits. A competent person should undertake the visits, which should include checks on:

- a) the validity of the assignment instructions; and**
- b) the satisfactory maintenance of records.**

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

This is a new requirement.

6.5 Performance evaluation

6.5.1 Contract performance monitoring

The organization should follow the recommendations for contract performance monitoring given in BS 10800:2020, 9.2.

A formal minuted meeting should take place with the customer to discuss contract performance against both the contract and the assignment instructions. In addition, the following items should be discussed:

- a) security officer familiarity with assignment instructions and service delivery;**
- b) security officer performance; and**
- c) security officer training needs.**

NOTE 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.

This is a new sub-clause.

6.5.2 Employee performance monitoring

6.5.2.1 Welfare check

Each security officer should receive a welfare check at least once a month from either a 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 and could include discussions on health and wellbeing, personal circumstances and security officer's concerns.

This is a new sub-clause.

6.5.2.2 Performance review

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

The following should be discussed:

- a) familiarity with assignment instructions and service delivery;**
- b) performance; and**
- c) training needs.**

If there have been changes to the security officer's duties or circumstances within the review period, confirmation of the security officer's understanding of the changes should be recorded.

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. These reports should form part of the annual performance appraisal.

Organizations should have processes in place that allow security officers to raise issues outside of the monthly welfare check.

This is a new sub-clause.

6.5.3 Annual performance monitoring

The organization should follow the recommendations for performance appraisal visits given in BS 10800:2020, 9.4.

This is a new sub-clause referring to BS 10800:2020.

6.6 Control of customer property

6.6.1 General

Customer property held, used or managed by the organization should be controlled and recorded in a secure manner that prevents misuse.

This is a new sub-clause.

6.6.2 Control and movement of keys on sites

Details of keys received at the commencement of an assignment should be recorded. When not in use, keys should be kept in a secure manner. Where a customer is unwilling to provide a secure manner for storing keys, the organization should document that it has recommended the use of a secure manner of key storage.

NOTE This may be a description of the key press or, where there is a large quantity of keys, an inventory uniquely referencing each key or set of keys.

Each set of keys should be stored ready for inspection at all times and should be uniquely referenced with its details recorded with the key press, or in an inventory.

Supervisory staff or management should check and confirm every three months that all stored keys match the inventory.

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

Where applicable, a list of individuals authorized to receive keys should be maintained.

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; and**
- d) the name of the issuing and receiving security officer.**

Where keys are removed from site in accordance with the assignment instructions and the customer's consent, the name of the security officer retaining the keys should be recorded in the key register and that security officer should sign to confirm receipt of them.

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.

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.

Where applicable, a list of individuals authorized to receive keys should be maintained.

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; and**
- d) the name of the issuing and receiving security officer.**

Where keys are removed from site in accordance with the assignment instructions and the customer's consent, the name of the security officer retaining the keys should be recorded in the key register and that security officer should sign to confirm receipt of them.

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.

This is a new sub-clause containing requirements to control and prevent misuse of all customer property, not just keys as required by the 2013 edition.

The sub-clause relating to keys on mobile patrols contained in the 2013 edition has moved to BS 7984-3.