Security.Improved

National Security Inspectorate

NSI Code of Practice for Design, Installation and Maintenance of Access Control Systems NCP 109

This Code of Practice is to be read in conjunction with the NSI Regulations relating to approval by NSI, the NACOSS Gold approval criteria and the Systems Silver approval criteria.
No company shall hold out or claim that it adheres to this Code, save by virtue of holding NSI approval, or having obtained the written permission of NSI.

NCP 109 (Issue 1)

July 2012

National Security Inspectorate

Code of Practice for the Design, Installation and Maintenance of Access Control Systems

This Code of Practice is in two parts.

Part 1 of this Code of Practice aims to assist purchasers, specifiers, installers and users in selecting the level of access control equipment best suited to a particular risk and to provide guidelines for the design and installation of access control systems.

Part 2 of this Code of Practice provides guidelines for the maintenance of access control systems installed as in Part 1.

This Code of Practice is provisional pending publication of a suitable British Standard.

Note: British European Standard BS EN 50133, although published in several Parts, has not been widely adopted.

LIST OF CONTENTS

In this document, material (such as guidelines, information, recommendations, advice) that does not form a mandatory requirement of this Code is shown in italics

FOREWORD

An electronic access control system consists of recognition equipment, such as a token and reader, electronically activated entrance release hardware and, in certain systems, means for central control and/or monitoring.

The objectives of this Code of Practice are to:

(i) Establish and maintain minimum standards for access control systems.

(ii) Provide a framework to assist purchasers, installers and users in establishing their requirements with suppliers.

(iii) Assist specifiers and users in determining the appropriate level of security required for a given application.

(iv) Assist system designers in meeting specifier or user requirements.

The successful operation of an access control system requires the active co-operation of the user in carrying out the necessary procedures carefully and thoroughly. The usefulness of the whole system and its security and social acceptability can be jeopardised by lack of care. This care has to extend to the security of credentials such as tokens and of information regarding the system, its design, installation and method of operation and to ensuring adequate maintenance, to preserve the security of access.

We draw your attention to:

The Equality Act 2010, which aims to protect disabled people and to prevent disability discrimination, and the Disability Discrimination Act 2005 (as amended), the Disability Equality Duty of which continues to apply.

Approved Document B of the Building Regulations, which covers fire safety.

Approved Document M of the Building Regulations, which covers access to and use of buildings.

BS 7273-4, Code of practice for the operation of fire protection measures - Part 4: Activation of release mechanisms for doors.

BS 7671, Requirements for Electrical Installations (also known as the "IET Wiring Regulations").

PART 1: CODE OF PRACTICE FOR DESIGN AND INSTALLATION

1. SCOPE

This Part of the Code of Practice contains requirements and recommendations for the design and installation of electronic access control systems classified by the degree of security provided.

Guidance:

a) Purely mechanical locking devices are outside the scope of this Code of Practice. There must be some electrical/ electronic components to the product.

b) Systems where a person makes the decision as to who may enter or exit are outside the scope of this Code of Practice.

Example: A door entry telephone system used in conjunction with an electrically-operated lock triggered by a person using a manual switch/button.

c) Where the entire system is housed within a single unit/housing located at the access point, with no signalling link to control equipment located away from the access point, the system does not need to meet this Code of Practice.

Note 1: A unit/housing containing a bolt or pin and the striking plate or box into which the bolt or pin is thrown is considered to be a single unit/housing.

Note 2: Electrical wiring, radio-links, laser-links, fibre-optic links, and mains-borne signalling are examples of signalling links (but refer to Note 3 below which allows an exemption for electrical supply failure auto-release facilities).

Note 3: The provision of an auto-release, such that the access point releases in the event of failure of an electrical supply system, is not regarded for the purposes of c) above as amounting to a signalling link to control equipment located away from the access point.

NSI NACOSS Gold and Systems Silver approved companies must comply with this Code of Practice (NCP 109).

NSI approved companies may, as an alternative to complying with NCP 109, comply with BS EN 50133-1:1997 and BS EN 50133-7:1999. However BS EN 50133 has not been adopted widely due to lack of available equipment.

2. DEFINITIONS

For the purposes of this Code of Practice the following definitions apply:

2.1 Access control system. An electronic system restricting entry into and/or exit from a controlled area.

2.2 Access control unit (ACU). A device which processes data from the reader to authorise or reject access to the secure area.

The ACU is usually installed near the access point.

2.3 Access level. User authority in terms of access to specified, controlled area(s).

2.4 **Access point**. The position at which access can be controlled by a door, turnstile or other secure barrier.

2.5 **Access point hardware**. Mechanical and/or electro-mechanical devices capable of releasing the access point.

2.6 **Biometric**. Any measureable, unique physiological characteristic or personal trait that is used as a credential to recognise and verify an individual.

Examples: Fingerprint, hand or face geometry, retinal/eye pattern, voice pattern or signature or keyboarding dynamics and so on.

2.7 **Central processor**. Equipment directing the functions of a number of ACUs, changing data for individual ACUs and/or monitoring an access control system.

2.8 **Common code**. A sequence of characters (alpha and/or numeric) unique to a particular keypad-operated access control system and memorised by every user of the system.

2.9 **Common token**. A token unique to a particular access control system, or reader, with all user tokens identical.

2.10 **Controlled area**. The area accessed by the presentation of a valid credential.

2.11 **Credential**. Any token or memorised information or biometric used to identify an individual to an access control system in order to verify user access.

2.12 **Equal Error Rate (EER) or Crossover Error Rate (CER)**. The rate at which accept and reject errors are equal.

See 2.15 and 2.16 below.

2.13 **Fail locked**. The securing of a locking mechanism at an access point in the event of identified system failures.

2.14 **Fail unlocked**. The release of a locking mechanism at an access point in the event of identified system failures.

2.15 **False Acceptance Rate (FAR)**. A measure of the likelihood that a biometric security system will incorrectly accept an invalid credential.

2.16 **False Rejection Rate (FRR)**. A measure of the likelihood that a biometric security system will incorrectly reject a valid credential.

2.17 **Keypad**. A data entry point for the input of a numeric or alphanumeric code into an access control system.

2.18 **Personal Identification Number (PIN) code**. A sequence of characters (alpha and/or numeric) allocated to and memorised by an individual user of an access control system.

A PIN code is unique to each user.

2.19 **Reader**. Equipment for the extraction of data from a token or a biometric.

2.20 **Radio-frequency identification** (**RFID**). The use of radio-frequency electromagnetic fields to transfer data from a token to a reader.

2.21 Tamper detection. A means for the detection of deliberate interference with a component of an access control system.

2.22 Time zone. A period of time during which system operating requirements are changed, such as refusal of access outside normal working hours or PIN override.

2.23 Token. A type of credential.

2.24 Transaction. A recognisable event occurring within an access control system, such as the release of a door following presentation of a valid credential or the generation of a door alarm report.

An example of a door alarm report would be an 'access point held open' alarm.

2.25 Unique token. A token which, in addition to any data common to all users of a particular access control system, carries some data allocated uniquely to the user of that token.

A unique token is individual to each user regardless of site.

Typically the data encoded within a unique token will have a minimum of eight numeric characters.

3. CLASSIFICATION OF ACCESS POINTS

3.1 General

Access points are classified by the requirements for successful legitimate access (see Class I, Class II, Class III and Class IV below). Classification is related to the level of security provided for each access point and the class can change according to the time of day or night.

For each class, access may be granted by the use of credentials permitted at higher classes, but not by the use of credentials permitted at lower classes.

You must determine the classification of each access point during the design stage (see Clause 4 below).

You must include the location and classification of each of the access points making up an access control system in the system design proposal and in the as-fitted document.

In all classes, data encoded within tokens must be protected against unauthorised change (for example by requiring an authorised person/manager to enter a password to gain access to software at the central processor to make changes).

In all classes, codes must be protected from repeated attempts to select the correct code (for example by limiting the number of attempts to a maximum).

Facilities to control readers from a central point, to record information regarding the access of individual token holders and to monitor the status of access points where this is required may be incorporated into any access control system.

Monitoring, 'access point held open' alarm, cable security and standby power operation are related to the level of security provided within a classification.

3.2 Class I (low risk)

At an access point to class I, access will only be granted following:

- The input of a correct common code (or the input of a correct PIN code) of not less than 10,000 differs.

  10,000 differs requires a 4 digit code number such as 1234.

3.3 Class II (low to medium risk)

At an access point to class II, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 1,000,000 differs;

  OR

- Option B - the presentation of a valid unique token to a reader.

  1,000,000 differs requires a 6 digit code number such as 123456.

3.4 Class III (medium to high risk)

At an access point to class III, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 10,000 differs AND the presentation of a valid unique token to a reader;

  OR

- Option B - the presentation of a valid biometric to a reader.

3.5 Class IV (high risk)

At an access point to class IV, access will only be granted following:

- Option A - the presentation of a valid biometric to a reader AND the presentation of a valid unique token using radio frequency identification (RFID)*;

  OR

- Option B - the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs.

  * *RFID must not rely on recognising the Chip Serial Number (CSN) only. Also the code to be read must be stored in the memory of the card.*

4. DESIGN

4.1 Survey

The importance of a correct and adequate survey for installation is paramount.

You must ensure that all staff visiting premises are security screened to BS 7858

and carry identification cards, which must include a photograph of the bearer, their signature, the name of your company and a date of expiry.

Where relevant, you should consult with relevant managers such as those responsible for information technology and human resources at the customer's premises.

Access point design has a substantial bearing on the performance and reliability of an access control system.

Access points must not:

- conflict with fire regulations
- restrict exit in such a way as to endanger people in an emergency

You must consider the following aspects when designing an access control system:

- how access points will operate in the event of mains power failure and the period, or number of transactions, required in such circumstances;
- whether access points should fail locked or fail unlocked;
- whether secondary non-controlled locking devices should be fitted on external doors that fail unlocked;
- whether a key override is required for any critical doors to facilitate access in an emergency;
- whether ACUs will retain data in the event of data bus or power failure until the central computer or processor is operational;
- whether standby power is needed for the database (for example if held on a computer) to maintain its integrity during power failure;
- the choice of access control technology to provide an appropriate level of security for the risk to be protected;
- the choice of electronic equipment and its siting, taking into account environmental conditions and the potential for vandalism;
- the selection of access point hardware, taking into account the volume of traffic, environmental conditions and the level of physical security required;
- the numbers of users, access levels and time zones required, taking into account both present and predicted numbers of users and their needs;
- whether certain equipment needs to be protected against malicious damage;
- the need to site equipment such as controllers and printers in a secure area;
- the number of access points required, taking into account peak periods of use;
- whether an existing customer local area network (LAN) should be used;
- ease of access to ACUs and power supplies for preventative and corrective maintenance.

4.2 Equipment selection and installation

Except where otherwise specified, you must select and install equipment to withstand the following air temperatures:

Internally sited equipment, 0 ºC to +40 ºC

Externally sited equipment, -20 ºC to +50 ºC

Wider temperature ranges may be specified for some commercial, industrial and/or military applications.

Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. When the temperature is not well maintained internally in premises, temperature may vary between -10 ºC to +40 ºC and you should consider using equipment suitable for external use or similar. In all cases equipment should be suitable for use in the environment in which it is installed.

You must use environmental housings according to BS EN 60529 so as to afford appropriate protection (for example to IP54 or IP65 as applicable) where the possibility of penetration by solid objects, dust or water exists.

4.2.1 Credentials

Credentials may be thought of in terms of something you know (code), something you have (token) or something you are (biometric).

The security, size and durability of a credential are dependent upon the technology used to encode it and the equipment required to read it.

Credential technology should be selected as appropriate to the risk being considered and the needs of the customer.

Several types of credential are available including:

(a) memorized information such as common codes and PIN codes, which are input by hand to a keypad;

(b) magnetic token, including Wiegand effect;

Where magnetic tokens are powerful enough to corrupt other magnetically stored data in their immediate vicinity they should carry a printed warning to this effect. Limited life cards, for example cards carrying bank data, should not be used as access control tokens without prior agreement to this by the issuing authority.

(c) infra-red token;

(d) hologram token;

(e) proximity tokens using technologies such as radio or induction to allow the encoded data to be read within a specified operating range;

(f) biometric.

When selecting a battery powered active token you must take into account the life span of the battery and the environment in which the token will be required to operate and the frequency of its use.

4.2.2 Readers

You must provide a reader or controller and/or its associated access point hardware or a central control with the following features:

- an indication for access granted.
- variable time available for access to be made.
- tamper detection to detect access to the lock in circumstances where the lock can then be controlled from the insecure side.
- response within 2 seconds of the valid completion of the necessary data entry associated with the credential.

  Processing of more complex data such as those associated with biometric credentials may take longer than 2 seconds and this is acceptable provided the length of time is appropriate to the needs of the customer.

- re-locking of an access point if it is not used within a predetermined time.

When biometrics are used, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) should be balanced to reflect the need for security on the one hand and the need for operability on the other hand. If the FAR is high then it will be more likely that an unauthorised person will be able to gain access using their biometric. Accordingly, you should not normally provide the customer with the means to adjust biometric readers as this could seriously weaken the security of the access control system.

Just as a guide, the following may be typical for a biometric such as a finger print reader:

EER <0.01%
FAR <0.0001%
FRR <0.01%

If you do provide the customer with means to adjust biometric readers then access to the means of adjustment must be protected against unauthorised change (for example by requiring an authorised person/manager to enter a password) and you must provide the customer with sufficient information to enable them to understand the consequences of making adjustments.

For example, you might provide the customer with information about the adjustments of their biometric readers that are acceptable and/or unacceptable for their security application.

You must mount readers:

- securely in position.
- adjacent to their access points and in positions convenient for all users to use, including those with disability.

We draw your attention to The Building Regulations 2000: Approved document M: access to and use of buildings.

4.2.3 Access point hardware

You must select access point hardware:

a) In accordance with the degree of physical security and the anticipated

number of users and the duty cycle of the access point to which they are fixed;

b) With regard to the following, particularly when planning to use mechanisms externally:
   - temperature
   - humidity
   - corrosion
   - vibration
   - dust and other contamination
   - physical abuse

c) Taking into account the following with regard to the nature of the access point:
   - the existing physical strength of the access point, such as doors and frames.
   - the transfer of electrical connections onto doors must be via suitable flexible cables or other means of adequate reliability.
   - appropriate hardware must be used where rebated and double-rebate doors are controlled.
   - necessary safety precautions must be taken where all-glass or other special doors are controlled.
   - door closing devices must be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.

     Where adverse air pressure exists, you should provide means for relief of the air pressure.
   - doors must be a satisfactory fit in the frame.
   - hinges, frame and fixings must be adequate for the weight and proposed usage of a door.

     You should follow manufacturers' recommendations for turnstiles and similar barriers, and their release mechanisms.
   - where manual or automatic override features are used, continuously rated releases will be required.

Access point hardware alone may not provide sufficient physical security in some circumstances.

The degree of physical security is related to the classification of access points. An access point to a higher class will usually require greater physical security than an access point of a lower class.

You should select the necessary locking mechanisms to be appropriate to the strength of the door and its frame and you should not reduce the physical strength of the access point significantly when fitting the mechanisms.

As a guide, powered locks should have the following holding forces according to the class of the access point:

Class I	*Holding force = 3 kN or more*
Class II	*Holding force = 5 kN or more*
Class III	*Holding force = 7 kN or more*
Class IV	*Holding force = 10 kN or more*

kN = kilonewtons, 1 kN = 1,000 newtons

You should reinforce the physical strength of an access point if this is likely to be unduly reduced by the attachment of the access control hardware. If the customer will not let you do this, you should confirm the facts of the situation in writing to the customer.

Where access point monitoring is of critical importance, you should consider monitoring the locked / unlocked state of the access point, in addition to any monitoring by means of a separate protective switch.

Locking mechanisms can have two modes of operation under system failure conditions, 'failed unlocked' and 'fail locked'. Where exit is available by purely mechanical means, the fail locked mode may be acceptable but where exit is granted by electrical means, the 'fail unlocked' mode may be mandatory to meet safety legislation.

In the case of a complete power failure it may be necessary to provide a key override to a critical door (or doors) with the key (or keys) kept in a safe place outside the controlled door (or doors).

The suitability of any access control system must be considered in relation to the fire risk assessment for the premises and the need for safe exit in emergency situations.

Where applicable, you must agree on what methods are to be used to release all the access points (for example green coloured single action emergency exit buttons, or break glass units, on the secure sides of access points) and you must document these methods in the system design proposal and the as-fitted document.

4.2.4 Power supplies

You must select the power supply to meet the largest load likely to be placed upon it under normal operational conditions.

All equipment housings shall be clearly marked with the operating, or supplied, voltage.

Where the power supply is separate from the ACU, the voltage input to ACUs must not exceed 50 V.

Certain release mechanisms associated with an access control system, such as those for roller shutters, may operate at mains voltage and specific electrical safety requirements will apply to these.

Where safety and security considerations do not require continued operation of a system during a mains supply failure, the public mains supply via a safety isolating transformer may be the sole supply for the system. A 'clean' source for this may be required in electrically noisy environments.

You must:

- locate power supply units within controlled areas and in positions secure from tampering;
- provide additional security for power supply units that incorporate fail unlocked hardware;
- connect the mains power supply permanently to the access control system via a fused outlet, not by plug and socket;
- not bring extra low voltage cables into a power supply container through the same entry point as any mains cables (except where impractical to avoid doing so).

Where continued operation of the access control system is essential during mains supply failure, a standby power supply must be used having the necessary capacity to support the system for not less than the minimum period as agreed with the customer.

4.2.5 Cables

4.2.5.1 Where practicable, you must install cables within controlled areas.

Where practicable, cables should be concealed.

Where cables are exposed to possible mechanical damage or tampering, or are outside controlled areas, they must be protected by suitable conduit, trunking, or armour. Where an access point release signal passes outside of a controlled area, metal conduit (or equivalent protection) must be used.

All interconnecting wiring must be supported and its installation must conform to good working practice.

All extra low voltage cable joints must be made in suitable junction boxes using either soldered, crimped, or screw-terminals. Alternatively plugs and sockets can be used provided fire safety is not compromised.

Extra low voltage signal cables must not run in close proximity to mains power cables or other low or high voltage cables.

4.2.5.2 Signal cables for the transmission of data or other low level signals must be of a type and size compatible with the rate of data transfer and anticipated levels of electromagnetic interference.

4.2.5.3 Low voltage cables from both mains and standby power supplies to remote equipment shall be of sufficient rating to permit satisfactory operation of the equipment at the end of any proposed length of cable run.

4.3 Control

You must consider the following when selecting controls:

- operational requirements of the associated controllers;
- protection against unauthorised interference with the system database or programme;
- logging of transactions;
- annunciation of alarms;
- blocking, validation and deletion of tokens;
- database for the retention of token holder details with back-up copies of corruptible data to facilitate re-establishment of the system in the event of a

failure;

- programming of access levels and time zones;
- period of operation following mains failure and/or storage of data by non-volatile means;
- ease of access for maintenance and serviceability.

Control may be by means of a proprietary computer.

You must adhere to the manufacturers' specified environmental conditions, particularly in respect of:

- temperature;
- humidity;
- dust and other air contamination;
- vibration;
- electromagnetic interference.

You must take into consideration the following when siting control equipment:

- ventilation;
- access for maintenance;
- user access for archiving and so on;
- noise from associated printer;
- physical security and supervision;
- general visibility to unauthorized people of any displayed data.

5. COMMISSIONING, HANDOVER AND DOCUMENTATION

5.1 Commissioning

You must check the following during commissioning:

- all wiring is correctly terminated;
- voltage and resistance at all appropriate points of the system are correct, which must be recorded;
- alignment and operation of access point hardware and of release and closure mechanisms at each access point is correct;
- emergency release mechanisms at all the access points are in full working order;
- operation of each reader is correct;
- release time for each door is correct;
- door held open signal, if specified, is present;
- correct authorisation of access is verified by the input of appropriate data;
- access control system continues to work when mains supply disconnected (if specified).

5.2 Handover

At handover, you must:

- provide a system log book to the customer and explain how to record/report problems;
- demonstrate all aspects of the system operation to the customer, including any necessary safety precautions and any standby power facilities;

- ensure that the correct documentation (see 5.3) is given to the customer to enable the system to be operated, adjusted and maintained;
- train the users in the correct operation of the system and arrange for any further training if necessary;
- for PC based systems, train the users on how to produce a system back-up and recommend that back-ups are carried out on a regular basis.
- ensure that users know the procedure for summoning assistance in the event of system malfunction;
- instruct the customer to establish whether personal information held within the system requires registration under the Data Protection Act.

Where an access control system is managed remotely, you should include details of this in the documentation (see 5.3), for example the method of control and where control is carried out.

5.3 Documentation

Upon completion of installation of the access control system you must produce an as-fitted document including the following information:

(a) the name, address and telephone number of the controlled premises;

(b) the name, address and telephone number of the customer;

(c) the location and classification of each access point and the type and location of each controller and its associated hardware (for example the type of token/reader technology);

(d) the type and location of power supplies;

(e) power supply standby periods where relevant;

(e) details of those access points which the customer has the facility to override;

(f) the type and location of any warning device;

(g) details and settings of any preset or adjustable controls incorporated into the system;

(h) relevant documentation relating to equipment;

(i) relevant documentation relating to software functions;

(j) the number of keys, codes, tokens, and so on for the system provided to the customer;

(k) details of the methods adopted for emergency override for safe escape.

You must agree the as-fitted document with the customer and provide the customer with a copy.

You may provide some of the information required for the as-fitted document in the form of a diagram of the installed system.

You should advise the customer to keep all documentation for the access control system in a place where access is restricted to authorized people.

For PC based access control systems, the software media may be handed over to the customer for safe keeping on site for use during service visits if required. A back-up of the initial system configuration (which may also include a copy of the database records) may also be handed over to the customer for system recovery if necessary.

PART 2: CODE OF PRACTICE FOR MAINTENANCE AND RECORDS

1. SCOPE

This Part of the Code of Practice contains requirements and recommendations for the preventative and corrective maintenance of, and keeping of records for, access control systems, installed in accordance with Part 1 of this Code.

2. DEFINITIONS

The definitions given in Part 1 of this Code apply, together with the following definitions.

2.1 Maintenance

2.1.1 Maintenance company. An organisation providing maintenance of an access control system.

2.1.2 Preventative maintenance. Routine servicing of an access control system, carried out on a scheduled basis.

2.1.3 Corrective maintenance. Emergency servicing of an access control system, or part thereof, carried out in response to the development of a fault.

2.2 Commissioning. The completion of installation and final checking of an access control system prior to its handover.

3. MAINTENANCE

3.1 General

3.1.1 *It is advisable that you as the installing company should also carry out the maintenance.*

Whatever arrangements are made, you as the maintaining company must have the means, including spare parts and documentation (see 5.3 of Part 1), to comply with this Part of the Code.

This recommendation does not place an obligation upon customers to have their access control systems maintained; maintenance is a matter of agreement between you and the customer or between the customer and a separate maintenance company.

Where a PC based system is installed, you should advise the customer to consider having a software support agreement with the software supplier so that updates to the software and technical support are provided. This is unless you are maintaining the system and providing the necessary software and support.

3.1.2 You must ensure the safe custody of all equipment and documentation pertaining to installations and within your control.

3.1.3 Each service technician you employ must carry a range of tools, test instruments and other equipment to enable them to perform their functions satisfactorily. Specialist tools, test equipment and plant must be available for deeper investigation as necessary.

Not all eventualities can be foreseen and, in exceptional circumstances, a system or part(s) of a system may have to be left inoperable or disconnected whilst tools or replacement components are obtained (see 4.6).

3.1.4 Your organisation must be staffed so as to ensure that the requirements of this part of the Code can be met at all times. You must take the following factors into consideration the:

(a) number of installations to be serviced;

(b) complexity of the installations;

(c) geographical spread of the installations in relation to the location of the maintenance company, its branches and its service personnel;

(d) method of calling out service personnel outside normal office hours.

3.1.5 Service personnel must be adequately trained and training must be updated whenever appropriate.

3.2 Preventative maintenance

3.2.1 Frequency of visits

Your representative must make preventative maintenance visits to the controlled premises during or before the twelfth calendar month following the month of commissioning or of the previous preventative maintenance visit.

The mechanical components in an access control system such as locks and hinges will require routine preventative maintenance by the user more frequently than once per year.

3.2.2 Inspection

3.2.2.1 During each preventative maintenance visit, inspection of the following, with all necessary tests, and those rectifications which are practical at the time, must be carried out:

(a) the installation, location and siting of all equipment and devices against the as-fitted document (see 4.2);

(b) the satisfactory operation of all equipment;

(c) all flexible connections;

(d) the normal and standby power supplies, for correct functioning;

(e) the control equipment, in accordance with your procedure;

(f) the operation of any warning device in the system.

3.2.2.2 Those items of inspection and rectification which are not carried out during the preventative maintenance visit must be completed as soon as practicable.

3.2.2.3 Those parts of a system or any environmental conditions which are found during preventative maintenance to be the potential cause of reduced security must be identified on the maintenance visit record (see 4.4).

3.3 Corrective maintenance

3.3.1 An emergency service must be available and the customer must be kept informed of the address and telephone number for your company's emergency service facility.

3.3.2 You must locate and organise the emergency service facility so that, except under abnormal circumstances, your representative reaches the controlled premises within the period agreed to in writing with the customer.

4. RECORDS

4.1 General

You must establish, retain and maintain a system of records relating to the access control systems you maintain including the information required by 4.2 to 4.6. It is essential that these records are protected from unauthorised access.

We draw your attention to the Data Protection Act in those cases where records contain information concerning individuals.

4.2 As-fitted document

An as-fitted document will have been generated at installation and may include previous information from the system design specification, as well as that required by 5.3 of Part 1. You must keep this document up to date and the document must be available to your maintenance technician for each maintenance visit.

The updated as-fitted document does not need to include the number of keys, codes, tokens and so on where the customer has control of these.

The system information as required by Part 1 of this Code may be provided in diagrammatic form.

4.3 Historical record

You must keep a historical record with the date of every visit, any faults found and the action taken. Details of every fault reported to you must be included, together with details of any action taken, and, if known, the cause.

You must keep this information for at least 2 years after the last event to which it refers.

4.4 Preventative maintenance record

You must enter the results of a preventative maintenance inspection on a maintenance visit record. A record of checks and work carried out should either be given to the customer at the time of maintenance or provided within 10 days.

This record may be in electronic form if acceptable to the customer.

You must keep this information for at least 15 months after the inspection to which it refers.

4.5 Corrective maintenance record

You must keep a record of the date and time of receipt of each request for emergency service, together with the date and time of completion of corrective maintenance and the necessary action(s) carried out.

You must keep this information for at least 2 years after the emergency call to which it refers.

You must enter the result of a corrective maintenance inspection on a maintenance visit record. A record of checks and work carried out should either be given to the customer at the time of maintenance or provided within 10 days.

This record may be in electronic form if acceptable to the customer.

You must keep this information for at least 15 months after the inspection to which it refers.

If a preventative maintenance inspection is made at the same time as the corrective maintenance visit, you should complete separate visit records.

4.6 Temporary disconnection record

You must keep a record of any temporary disconnection of the system or of any component part(s) of it. This must identify which part(s) of the system and the associated equipment is not operable. You must give the reason for the disconnection and the date and time of disconnection and of subsequent reconnection. You must obtain a signed authorization for each disconnection from the customer or their representative.

You must keep this authorization for at least 3 months after reconnection.

National Security Inspectorate
Sentinel House, 5 Reform Road
Maidenhead, Berkshire SL6 8BY
Telephone: 01628 637512 or 0845 006 3003 Fax: 01628 773367
E-mail: nsi@nsi.org.uk
Web: www.nsi.org.uk