Code of Practice
for Planning, Installation and
Maintenance of Access Control Systems
ICP 30

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

NSI SYSTEMS SILVER

Issue 2
26th June 2003

© NSI Copyright. No part to be reproduced without permission of NSI

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

LIST OF CONTENTS

PART 1: CODE OF PRACTICE FOR PLANNING AND INSTALLATION

1. SCOPE

2. DEFINITIONS

3. ACCESS POINT CLASSIFICATION

4. SURVEY

5. COMMISSIONING, HANDOVER OF DOCUMENTATION

PART 2: CODE OF PRACTICE FOR MAINTENANCE AND RECORDS

1. SCOPE

2. DEFINITIONS

3. GENERAL MAINTENANCE

4. RECORDS

Note 1: This Code of Practice is in two parts.

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

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

Note 2: This Code of Practice is regarded as PROVISIONAL pending publication of a British Standard.

Note 3: NSI Systems Silver wishes to acknowledge that the technical content of this Code of Practice is based on material prepared under the auspices of the British Standards Institution. Such material is used by permission.

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

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:

(i) *The establishment and maintenance of minimum standards of installation for access control systems.*

(ii) *The provision of a framework to assist purchasers, installers, and users in establishing their requirements with suppliers.*

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

(iv) *The assistance of system designers in meeting specifier of user requirements.*

(v) *The establishment of definitions for terms used within the access control industry.*

(vi) *The establishment of minimum standards of maintenance for installed access controlled systems.*

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 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.

Attention is drawn to the Regulations for Electrical Installations (15th Edition) published by the Institution of Electrical Engineers and to MPT1337 and MPT1339 (DTI Radiocommunications Division).

PART 1: CODE OF PRACTICE FOR PLANNING AND INSTALLATION

1 SCOPE

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

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 **Controlled area**. The area accessed by the presentation of valid recognition data.

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

2.4 **Access point hardware**. Mechanical and/or electro-mechanical devices at an access point enabling its release by an authorised user.

NOTE: Access point hardware makes no decision regarding the permitting or refusal of access.

2.5 **Access level**. User authority in terms of access to specified, controlled area.

2.6 Token. A device containing encoded recognition data.

NOTE: This includes a human being as the source for biometric data.

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

2.8 System token. A common token encoded additionally with specific system identification data.

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

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

2.11 Personal identification number (PIN). A sequence of characters allocated to an individual user of an access control system keypad.

2.12 Common code. A sequence of characters unique to a particular keypad-operated access control system and allocated to every user of the system.

2.13 Reader. Equipment for the extraction of recognition data from a token.

2.14 Biometric system. An access control system using recognition of a physiological characteristics of the user, such as fingerprints, retinal pattern, voice pattern or signature.

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

2.16 Controller. A device which processes recognition data to enable usable output conditions to be derived.

2.17 Central control. ('On-line') Equipment directing the functions of a number of controllers, changing data for individual controllers and/or monitoring an access control system.

2.18 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.

2.19 Fail locked. The securing of a locking mechanism in the event of identified system failures.

2.20 Fail unlocked. The release of a locking mechanism in the event of identified system failures.

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

3. ACCESS POINT CLASSIFICATION

3.1 General

Access points are classified by the requirements for successful legitimate access i.e., the level of security provided. The installing company shall indicate to the customer the classification of the access points making up an access control system, related to the level of security provided.

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

NOTE: 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 - Common code

At an access point to class I, access will only be granted following the input of a correct common code. The code shall be numeric, alphabetic, or a combination of both, with a minimum of four digits and/or characters. The code used shall be one of not less than 1000 differs and shall be protected against unauthorised change and repeated attempts to select the correct code.

3.3 Class II - Common token

At an access point to class II, access will only be granted following the presentation of a valid common token to a reader and when the code within the token is recognised by the system. Each token shall have the same encoded date chosen from a minimum of 10,000 differs. The code shall be protected against unauthorised change.

3.4 Class III - System token

At an access point to class III, access will only be granted following the presentation of a valid system token to a reader. The token shall be encoded with a system code of not less than 200 differs and an individual code of not less than 10,000 differs. The codes shall be protected against unauthorised changes.

NOTE 1. Tokens can be added to or deleted from the system.
NOTE 2. System tokens should not be acceptable to other systems in the same geographic area unless specifically intended to be so.

3.5 Class IV - Unique token

At an access point to class IV, access will only be granted following the presentation of a valid unique token to the reading device. The token shall be encoded with a minimum of 10 million differs. The code shall be protected against unauthorised change.

NOTE: Tokens can be added to or deleted from the system.

3.6 Class V - Unique token and PIN

At an access point to class V, access will only be granted following the presentation of a valid system token (see class IV) and the input of a correct personal identification number of not less than four characters.

4. PLANNING

4.1 Survey

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

Access point design has a substantial bearing on the performance and reliability of an access control system and the following aspects shall be considered when planning an access control system.

- Access points shall not conflict with fire regulations and shall not restrict exit in such a way as to endanger persons in an emergency.

- The operation of access points 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.

- 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 sitting, taking into account environmental conditions such as weather 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 future levels.

- The need for siting of equipment such as controllers and printers in a secure area.

- The number of access points required, taking into account peak traffic periods.

NOTE: Advice concerning physical security is given in BS 8220.

4.2 Equipment selection and installation

Equipment shall be selected and/or installed to withstand the following air temperatures:

Internally sited equipment, 0^{o} to 40^{o}C

Externally sited equipment, -20^{o} to 50^{o}C.

NOTE: Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. Exterior equipment should be considered for use in unheated premises.

Where equipment is exposed it shall meet IP54 or, in a particularly exposed location, IP65 as specified in BS 5490; necessary apertures in equipment are exempt from these requirements at such points.

4.2.1 Tokens

The security, size and durability of a token is dependent upon the technology used to encode it and required to read it.

Several types of token are available including:

(a) magnetic, including Wiegand effect;

NOTE: 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 and limited life cards e.g., those carrying bank data, should not be used as access control tokens without prior agreement to this by the issuing authority.

(b) infra-red;

(c) Holograms;

(d) Proximity devices using technologies such as radio or induction to allow the code to be read within a specified operating range;

(e) Biometric i.e., a specific person or their signature. Token technology

should be selected appropriately to the risk being considered.

The choice of size and durability of a token and the life span of a battery powered active token shall take into account the environment in which it will be required to operate and the frequency of its use.

4.2.2 Readers

A reader or controller and/or its associated access point hardware or a central control shall provide the following features:

- An indication for access granted.
- Variable time available for access to be made.
- Detection of physical tampering and, for readers fitted externally, protection against malicious damage.
- Response within 2 s of the valid completion of the necessary entry procedure(s) and re-locking of an access point if it is not then used within a predetermined time.

Readers shall be securely mounted in a convenient position for the user adjacent to the access point.

NOTE: Proximity readers may be sited at any point where successful activation will occur.

4.2.3 Access point hardware

Mechanisms shall be selected in accordance with the degree of security, related to the classification, and the anticipated traffic and duty cycle of the access point to which they are affixed.

NOTE: Access control hardware alone may not provide sufficient physical security in some circumstances.

Access point hardware shall be carefully selected with regard to the following, particularly when planning to use mechanisms externally.

- Temperature
- Humidity
- Corrosion
- Vibration
- Dust and other contamination
- Physical abuse

The selection of access point hardware shall take account of the following with respect to the nature of the access point as follows:

- The existing physical strength of the access point, such as doors and frames, *which should not be significantly reduced by the fitting of the necessary locking mechanisms and the mechanism should be selected appropriately to the strength of the door frame.*

NOTE: The physical strength of an access point should be reinforced if this is likely to be reduced by the attachment of the access control hardware; advice on the physical strength requirements is given in BS 8220.

- The transfer of electrical connections onto doors via suitable flexible cables or other means of adequate reliability.
- Appropriate hardware where rebated and double-rebate doors are controlled.
- Necessary safety precautions where all-glass or other special doors are controlled.
- Door closing devices shall be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.

NOTE: Where adverse air pressure exists means for its relief should be provided.

- Doors shall be a satisfactory fit in the frame.
- Hinges, frame and fixings shall be adequate for the weight and proposed usage of a door.

- *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.

Where access point monitoring is of critical importance, consideration should be given to monitoring the state of securement of the access point, i.e., closed and locked, 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.

NOTE: The suitability of any proposed access control system should be discussed with the local Fire Prevention Officer and it should be ascertained whether a central controller is an acceptable means of releasing access points in the event of an emergency, i.e., whether it is acceptable for a computer command to carry out this function.

4.2.4 Power supplies

The capacity of the power supply shall be selected to meet the largest load likely to be placed upon it under normal operational conditions. The operating voltage shall not exceed 50 volts.

NOTE: 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 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.

System power supplies shall be located within the controlled area in a position secure from tampering.

Systems incorporating fail unlocked hardware shall be provided with additional security for the power supply unit.

The main supply shall be permanently connected via a fused outlet i.e., not by a plug and socket.

Lower voltage cables shall not be brought into a power supply container through the same entry point as any mains cables.

Where continued operation of the system is essential during mains supply failure, a standby power supply shall be used having the necessary capacity to support the system for not less than the minimum period required by the customer.

4.2.5 Cables

4.2.5.1 Where practicable, cables shall be installed within a controlled area.

Where practicable, cables should be concealed.

Where cables are exposed to possible mechanical damage or tampering, or are in public areas, they shall 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) shall be used.

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

Any cable joints shall be made in suitable junction boxes using either wrapped, soldered, crimped, or screw-terminals.

Low voltage and signal cables shall not run in close proximity to mains or other transient carrying cables.

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

4.2.5.3 *Cables should be installed in accordance with IEE Regulations for Electrical Installations.*

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

4.3 Control

In selecting controls, consideration shall be given to the following:

- 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.
- Maintenance and serviceability.

Control may be by means of a proprietary computer.

The manufacturer's specified environmental conditions shall be provided, particularly in respect of:

- Temperature
- Humidity
- Dust and other air contamination
- Vibration
- Electromagnetic interference

The following shall be taken into consideration when siting control equipment:

- Ventilation
- Access for maintenance
- User access for archiving etc.
- Noise from associated printer
- Physical security and supervision
- General visibility to unauthorized persons of any displayed data.

5. COMMISSIONING, HANDOVER AND DOCUMENTATION

5.1 Commissioning

Commissioning shall include testing of the following aspects of the system:

- All wiring is correctly terminated.
- Voltage and resistance at all appropriate points of the system, which shall be recorded.
- Correct alignment and operation of access point hardware and of release and closure mechanisms at each access point.
- Correct operation of each reader.
- Release time for each door.
- Door held open signal, if specified.
- Verification of access levels, where specified, by the input of appropriate data.
- Ensure system continues to work when mains supply disconnected (if specified).

5.2 Handover

At handover, the installing company shall:

- 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.
- Ensure that the correct documentation (see 5.3) is given to the customer to enable to system to be operated, adjusted and maintained.
- Train the system user(s) in its correct operation and arrange for any further necessary training.
- 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.

5.3 Documentation

Upon completion of installation of the access control system there shall be a system record, which shall include 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;

(d) the type and location of power supplies;

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

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

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

(h) any documentation relating to equipment;

(i) the number of keys, codes, tokens, etc. to the system provided to the customer.

The system record shall be agreed with, and authorized by, the customer and a copy provided to the customer.

NOTE 1. Some of the information required for the system record may be provided by means of a diagram of the installed system.

NOTE 2. All documentation referring to a system should be kept in a place access to which is restricted to authorized persons.

PART 2: CODE OF PRACTICE FOR MAINTENANCE AND RECORDS

1. SCOPE

This Part of this Code of Practice contains recommendations and requirements 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

For the purposes of this Part of this Code of Practice the definitions given in Part 1 apply, together with the following definitions.

2.1 Maintenance

2.1.1 Maintenance company. An organisation prepared to maintain an installed system.

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

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

2.2 Commissioning. The completion of installation and final testing of a system prior to its handover.

3. MAINTENANCE

3.1 General

3.1.1 *It is advisable that maintenance should be carried out by the installing company.*

Whatever arrangements are made, the maintenance company shall have the means, including spare parts and documentation (see 5.3 of Part 1), to comply with this Part (Part 2) of this Code.

NOTE: This recommendation does not place an obligation upon customers who purchase their systems to have them maintained by the installing company; maintenance is a matter of agreement between the customer and the installing company or a separate maintenance company.

3.1.2 The preservation of security within the maintenance company is of paramount importance and steps shall be taken to ensure the safe custody of all equipment and documentation pertaining to installations. A maintenance company shall ensure that adequate vetting of employees is carried out and that all employees carry identification cards which shall include a photograph of the bearer, his signature, the company's name and a date of expiry.

3.1.3 Each service technician employed by the maintenance company shall carry a range of tools, test instruments and other equipment to enable him to perform his functions satisfactorily. Specialist tools, test equipment and plant shall be available for deeper investigation as necessary.

NOTE: 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 The maintenance company's organisation shall be so staffed as to ensure that the recommendations and requirements of this Part of this Code can be met at all times. The following factors shall be taken into consideration:

(a) the number of installations to be serviced;

(b) the complexity of the installations;

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

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

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

3.2 Preventative maintenance

3.2.1 **Frequency of visits**

Preventative maintenance visits to the protected premises shall be made by a representative of the maintenance company during or before the twelfth calendar month following the month of commissioning or of the previous preventative maintenance visit.

NOTE: 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, shall be carried out:

(a) the installation, location and siting of all equipment and devices against the system record (see 4.2);

(b) the satisfactory operation of all equipment;

(c) all flexible connection;

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

(e) the control equipment, in accordance with company 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 shall be completed within a period for 21 days.

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 reduce security, shall be identified on the maintenance visit record (see 4.4).

3.3 Corrective maintenance

3.3.1 An emergency service shall be available and the client shall be kept informed of the address and telephone number of the maintenance company's emergency service facility.

3.3.2 The emergency service facility shall be so located and organised that, except under abnormal circumstances, the maintenance company's representative reaches the controlled premises within the period agreed to in writing by the client.

4. RECORDS

4.1 General

The maintenance company shall establish, retain and maintain a system of records relating to the system including the information required by 4.2 to 4.6. It is essential that these records be protected from unauthorised access.

NOTE: Attention is drawn to the Data Protection Act, 1984 in those cases where records contain information concerning individuals.

4.2 System record

A system record 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. This shall be kept up to date and shall be available to the maintenance technician for each maintenance visit.

NOTE: The system information as required by Part 1 may be provided in diagram form.

4.3 Historical record

A historical record with the date of every visit, any faults found and the action taken shall be kept. Details of every fault reported to the maintenance company shall be included, together with details of any action taken, and, if known, the cause.

This information shall be kept for at least 2 years after the last event to which it refers.

4.4 Preventative maintenance record

The results of a preventative maintenance inspection shall be entered on a maintenance visit record and the signature of the client or his representative obtained on the record. A copy of the record shall be given to the client.

This information shall be kept for at least 15 months after the inspection to which it refers.

4.5 Corrective maintenance record

There shall be 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.

This information shall be kept for at least 2 years after the emergency call to which it refers.

The result of a corrective maintenance inspection shall be entered on a maintenance visit record and the signature of the client or his representative obtained on the record. A copy of the record shall be given to the client.

This information shall be kept for at least 15 months after the inspection to which it refers.

NOTE: If a preventative maintenance inspection is made at the same time as the corrective maintenance visit, separate visit records should be completed.

4.6 Temporary disconnection record

There shall be a record of any temporary disconnection of the system or of any component part(s) of it. This shall identify which part(s) of the system and the associated equipment is not operable. The reason for the disconnection and the date and time of disconnection and of subsequent reconnection shall be given. A signed authorization for each disconnection shall be obtained from the client or his representative.

This authorization shall be kept for at least 3 months after reconnection.

For additional information

about NSI Systems Silver please contact:

Sentinel House, 5 ReformRoad

Maidenhead, Berkshire SL6 8BY

Telephone 01628 637 512 Fax 01628 773 367

E-mail: nsi@nsi.org.uk Web www.nsi.org.uk