

# CODE OF PRACTICE

---

English Version

## **MONITORING AND ALARM RECEIVING CENTRE REQUIREMENTS**

**Final and agreed document**

**Dated: June 2005**

## **Foreword**

This Code of Practice has been prepared by a joint committee comprising members of CoESS and Euralarm

This Code of Practice shall be submitted to the relevant European Norm organisation as a discussion document to form the basis of a European Norm

| <b>Contents</b>                             | page      |
|---|-----------|
| <b>Introduction</b>                         | <b>4</b>  |
| <b>1. Scope</b>                             | <b>4</b>  |
| <b>2. Normative references</b>              | <b>4</b>  |
| <b>3. Definitions and Abbreviations</b>     | <b>5</b>  |
| <b>4. Inspection of MARC</b>                | <b>7</b>  |
| <b>5. Site Selection</b>                    | <b>7</b>  |
| <b>6. Construction</b>                      | <b>8</b>  |
| <b>7. Electronic Protection</b>             | <b>11</b> |
| <b>8. Communications</b>                    | <b>12</b> |
| <b>9. Reception of signals</b>              | <b>12</b> |
| <b>10. Power supplies</b>                   | <b>13</b> |
| <b>11. Manning and operating procedures</b> | <b>14</b> |
| <b>12. Data and Data Storage</b>            | <b>16</b> |
| <b>13. Alarm Handling</b>                   | <b>16</b> |
| <b>14. Emergency Planning</b>               | <b>17</b> |
| <b>Annex A</b>                              | <b>18</b> |

## **INTRODUCTION**

This Code of Practice applies to all monitoring and alarm receiving centres (MARC)s that monitor alarm systems that require an emergency response.

Alarms systems in communication with a monitoring centre shall comply with the applicable standard(s) for alarm systems current at the time of connection to the monitoring centre.

Alarm activities not falling within the scope of the applicable Standard(s) for alarm systems are excluded from this Code of Practice.

The alarm transmission system and the receiving centre transceiver, which is intended to be connected to the public and/or private telecommunication networks, shall be of an approved type for such connection.

It is noted that this Code of Practice cannot supersede any legislative requirements deemed necessary by a National Government to control this sector on a national basis.

### **1. SCOPE**

This Code of Practice specifies the requirements for the design, construction, manning, equipping and functioning of monitoring centres receiving signals from alarm systems.

### **2. NORMATIVE REFERENCE**

This Code of Practice incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred applies (including amendments).

EN 50136 - Alarm systems– Alarm transmission systems and equipment

EN 357 – Glass in building – Security glazing testing and classification of resistance against manual attack

EN 1522 – Windows, doors, shutters and blinds – Bullet resistance – Requirements and classifications

EN 1523 – Windows, doors, Shutters and blinds – Bullet resistance – Test methods

EN 12543 – Series – Glass in buildings – Laminated glass and laminated safety glass.

EN 13541 – Glass in building – Security glazing – Testing and classification of resistance against explosive pressure

### 3. DEFINITIONS AND ABBREVIATIONS

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

#### 3.1 Definitions

**3.1.1 Access:** Action of entry into or exit from a security controlled area.

**3.1.2 Alarm company:** An organisation, which provides services for alarm systems

**3.1.3 Alarm condition:** Condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard.

**3.1.4 Annunciation equipment:** Equipment located at an alarm receiving centre which displays the alarm status, or the changed alarm status of alarm systems in response to the receipt of incoming alarm messages.

**3.1.5 Alarm transmission equipment:** equipment which is primarily for the transmission of alarm messages from the supervised premises transceiver interface to the alarm system interface, to the receiving centre transceiver interface, to the annunciation equipment.

**3.1.6 Alarm transmission system:** equipment and network used to transfer information concerned with the state of one or more alarm systems to one or more receiving centres.

**3.1.7 Audible Verified:** An alarm signal verified by the MARC operator after having received audio information transmitted from the supervised premises and made a decision that it is considered a genuine intrusion or genuine attempted intrusion has occurred.

**3.1.8 Client:** Individual or corporate body with whom the MARC has entered into a contract to provide alarm monitoring services.

**3.1.9 Control and indicating equipment:** Equipment for receiving, processing, controlling and initiating the onward transmission of information.

**3.1.10 Deliberately Operated Device:** A device which, when manually operated, causes an alarm signal or message to be generated

**3.1.11 Detector:** A device designed to generate an alarm signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard.

**3.1.12 Fire resistance:** The ability of an element of building construction, component or structure to fulfil, for a stated period of time, the required stability,

fire integrity and/or thermal insulation and/or other expected duty in a standard fire resistance test.

**3.1.13 Fault condition:** A condition of an alarm system that prevents the alarm system or parts thereof from functioning normally.

**3.1.14 Intruder alarm system:** An alarm system to detect and indicate the presence, entry or attempted entry of an intruder into the supervised premises.

**3.1.15 Mains Power supply:** device(s) that provide and also modifies or isolates (electrical) power for the normal operation of a MARC or part thereof and for the storage device (e.g. a battery) if required.

**3.1.16 Monitoring:** The process of verifying that interconnections and equipment are functioning correctly.

**3.1.17 Monitoring centre:** an authorised, private or public place staffed 24 hours and which takes action on receiving the remote alarms from automatic intrusion or fire detection system.

Note: A monitoring centre may be separate to or part of an alarm receiving centre.

**3.1.18 Operator:** Person responsible for the handling of messages presented at the annunciation equipment.

**3.1.19 Receiving centre transceiver:** The alarm transmission equipment which is located at the receiving centre.

**3.1.20 Restore:** The procedure of cancelling an alarm, tamper, fault or other condition and returning the alarm system to a previous condition.

**3.1.21 Sequentially verified:** Signals emanating from two or more independent detectors which are configured such that it is considered a genuine intrusion or genuine attempted intrusion has occurred.

**3.1.22 Set:** The status of an alarm system or part thereof in which an alarm condition can be notified.

**3.1.23 Standby Power supply:** An energy source that is capable of supporting a MARC for extended periods.

**3.1.25 Supervised premises:** That part of a building and/or area in which a hazard may be detected by an alarm system.

**3.1.26 Unsecured door(s):** A door that is not secured by an electric or mechanical bolt in its fully extended, in the 'locked' condition.

**3.1.27 Unset:** The status of an alarm system or part thereof in which an alarm condition cannot be notified.

**3.1.28 Unwanted Alarm:** An alarm condition not generated by an intrusion or attempted intrusion onto the supervised premises.

**3.1.29 User:** Person(s) authorised by the client to operate an alarm system

**3.1.30 Visually verified:** An alarm signal verified by the MARC operator after having received a visual image(s) transmitted from the supervised premises and made a decision that it is considered a genuine intrusion or genuine attempted intrusion has occurred.

## **3.2 Abbreviations**

In this Code of Practice the following abbreviations are used:

|       |                                       |
|-------|---------------------------------------|
| ARC   | Alarm Receiving Centre                |
| CIE   | Control and Indicating Equipment      |
| CCTV  | Close Circuit Television              |
| EN    | European Norm                         |
| I&HAS | Intruder and Hold-up alarm System     |
| LEA   | Law Enforcement Agency                |
| MARC  | Monitoring and Alarm Receiving Centre |
| mm    | Millimetres                           |
| m     | Metre                                 |
| UPS   | Uninterrupted Power Supply            |

## **4. INSPECTION OF MARC**

The local law enforcement agency (LEA) shall have the right of inspection of the MARC. This inspection shall take place at any reasonable pre-arranged time.

## **5. SITE SELECTION**

**5.1 Site access.** The monitoring centre shall be contained within a building such that all areas of the building from which access to the monitoring centre's normal entrance can be gained are occupied by the company which operates the monitoring centre and which is the sole occupant. Such areas shall not be accessible to any other occupant of that building.

**5.2 Site accessibility.** There shall not be any entrances to such areas from any part of an adjoining premises except where those parts of such adjoining premises are also occupied by the company which operates the monitoring centre and which is the sole occupant. No part of such adjoining premises shall be accessible to any other occupant of that building.

**5.3 Site protection.** The area of the building occupied by the company which operates the monitoring centre, and in which the monitoring centre is located, shall be protected by an intruder alarm system installed in accordance with the applicable Standard(s) for intruder alarm systems. Such intruder alarm systems shall incorporate a

warning device to alert the monitoring centre staff immediately on activation of such a system.

**5.4 Site Occupancy:** For the purpose of the foregoing, the company which operates the monitoring centre may be deemed to include any other company trading exclusively within the security industry, where the control of such a company is exercised, either in whole or in part, by the same management as that of the actual company with whom clients contract for the provision of monitoring services.

## 6. CONSTRUCTION

**6.1 MARC Structure.** The monitoring centre structure shall consist of an enclosed room and connected lobby, the materials of construction of both of which shall comply with Table 1, or provide an equivalent level of security of construction. The enclosed room and connected lobby and the supporting structure shall have a fire resistance of at least 1-hour.

**6.2 Facilities.** Toilet and washing facilities should be provided within the MARC. Facilities for the preparation of food and drink should be provided and should be located within the MARC. Where a cooking appliance is provided it shall be separated from the operations area by a construction with a fire resistance of not less than 30 minutes.

**Table 1. Construction materials for monitoring centres**

| Construction elements   | Materials               | Dimensional or other requirements   |
|---|-------------------------|---|
| Perimeter walls<br>(including wall between station and lobby) | Solid masonry           | Minimum 200 mm thickness  |
|   | Concrete                | Minimum 150 mm thickness<br>20 MPa characteristic strength  |
|   | Solid steel             | Minimum 3mm thickness   |
| Internal Walls  | No requirements         | No requirement  |
| Floors on ground  | Concrete                | Minimum 150 mm thickness,<br>20 MPa characteristic strength.  |
| Suspended floors;<br>ceiling or roofs                         | Concrete                | Minimum 150 mm thickness,<br>20 MPa characteristic strength.<br>Depth and reinforcement<br>determined for span and<br>load conditions |
|   | Low carbon steel sheets | Minimum 1.5mm thick (sheets   |

|  |  |   |
|--|--|---|
|  |  | to be welded together and secured by non-returnable screws) |
|--|--|---|

(Note: The construction elements listed in Table 1 have been traditionally accepted as being able to resist attack. However, an equivalent level of security through resistance may be achieved using other construction materials.)

**6.3 Openings.** The only openings permitted in the structure of a monitoring centre shall be:

- the normal entrance (see clause 6.4);
- the emergency exit (see clause 6.6);
- glazed areas (see clause 6.7);
- ventilation (see clause 6.8);
- service inlets and outlets (see clause 6.9)

**6.4 The normal entrance.** The normal entrance shall comprise two doors, the dimensions of which shall not exceed 2.5m high by 1.1m wide, separated by a lobby the floor area of which shall not exceed 6m<sup>2</sup> and a minimum distance between both doors of 1.5m. The doors shall be interlocked to prevent both being opened at the same time except under controlled circumstances. The monitoring centre door to the lobby shall open into the lobby. The external lobby door shall always open outwards. Both doors shall have a fire resistance of at least one hour and shall be of substantial construction, such as either:

- (a) a solid hardwood door not less than 50 mm thick, or  
In the case of a hardwood door, the external door to the lobby shall be sheathed either on both sides with mild sheets each one of which shall be not less than 1.5mm thick, or with a single mild steel sheet not less than 3mm thick on one side or within the structure of the door. Where such sheet(s) are fitted to either or both faces of the door, they shall be secured with fixings such that those fixings cannot be removed externally.
- (b) A steel door incorporating not less than 6mm thickness of low - carbon steel.

Other forms of door shall be permitted only where they offer resistance to entry at least equivalent to (a) or (b) above, and where their design and construction comply with all other relevant sections of this Code.

The hinge edge of both doors shall have two fixed bolts of hardened steel or equal provision to prevent the door from being removed. It shall be possible for both doors, and the lobby interior, to be viewed from within the monitoring centre while both doors are secured. This requirement may be met through the use of door-viewers, closed-circuit television, or both. Both doors shall be fitted with an unlocking device normally

operable only from within the monitoring centre, and shall be fitted with automatic self-closing and locking devices. The doors shall be electrically interlocked to prevent both being unsecured at the same time. A means shall be provided within the monitoring centre to allow the locking devices to be overridden in the event of an emergency. The outer door lock shall be manually or electrically operable from within the lobby.

Any door furniture fitted to the external face of either door shall be of such type that it will not materially assist forcible entry. The construction of the door frame, and the fitting of the door to the door frame and the door frame to the structure, shall be such that the level of protection specified above shall be maintained.

**6.5 Electric lock/release mechanisms.** Any electric lock/release device fitted to the normal entrance lobby doors shall be mortice or rim-fitted. The boltwork or bolt receiver shall be electrically activated. The device shall deadbolt automatically when the door is in its frame. The fixing screws shall be protected against tampering while the door is in the closed position. There shall be a mechanical override for emergency release, protected against accidental use. In case of electrical failure, the bolt shall remain secure (i.e. locked). If the locking device is being fitted in the door, the electrical cable to the lock shall be contained in a metal armoured door loop, and otherwise be mechanically protected where exposed.

**6.6 The emergency exit.** Where a separate emergency exit exists the exit door(s), together with their hinges, frames, fixings, multiple locking points and unlocking devices, shall meet the same requirements for physical strength and resistance as those set down for an external normal entrance door to the lobby as specified in Clause 6.3. The exit door(s) shall open outwards and shall be provided with unlocking devices (e.g. panic bar) intended to be released only in the event of an emergency. The unlocking devices shall be operable only from inside the monitoring centre.

**6.7 Glazed areas.** Where glazed areas exist, their frames and fixing shall offer resistance to entry following physical attack at least equivalent to that provided by EN357 and EN1522. The interior of the monitoring centre shall not be visible through glazed areas from any point external to the outer building.

**6.8 Ventilation.** The cross-sectional area of ventilating inlets and outlets shall not exceed  $0.09\text{m}^2$  (300mm x 300mm nominal) each and it shall be ensured that the interior of the monitoring centre is not within the direct line of sight from the outer end of the ventilation duct. Where the cross-sectional area of a ventilating inlet or outlet exceeds  $0.02\text{m}^2$ , suitable alarm detection equipment shall be fitted to detect an attempt to enter the vent. Ventilation inlet and outlet openings in the shell of the monitoring centre shall be physically protected. Each vent shall be protected with an air-tight flap which can be locked in the closed position from inside the monitoring centre.

**6.9 Service inlets and outlets.** A breach in the shell of the monitoring centre for the admission of any service cable or pipe shall not exceed 0.02m in cross-sectional area. Infill material shall provide a resistance to physical attack or fire not less than that of the shell.

## **7. ELECTRONIC PROTECTION**

**7.1 General.** Security shall be such that the monitoring centre, including its external walls, doors and roof or ceiling are protected by an electronic protection system in accordance with the requirements stated below, and by an intruder alarm system installed in accordance with the applicable Standard(s) for intruder alarm systems. Where the monitoring centre is located other than at ground level, or where access may be gained from below (e.g. from a basement) then the floor of the monitoring centre shall also be protected by the electronic protection system. (See Table 1, Floors)

**7.2 Protection.** Detection devices shall be installed in accordance with the applicable Standard(s) for intruder alarm systems to detect forceful attack on the monitoring centre's structure. It is strongly recommended that the monitoring centre's phone lines should be protected by the electronic protection system such that the opening of the cover or door at the nearest Telecom service provider manhole or junction box through which the telephone service is provided to the monitoring centre is detected.

**7.3 Fire protection.** A fire detection system, installed according to the relevant standard, shall be provided for the protection of the monitoring centre. In addition, the monitoring centre shall have detection systems for at least carbon monoxide and smoke, which will give warning to the monitoring centre staff prior to levels reaching a concentration necessitating evacuation.

**7.4 Lightning protection.** The building housing the MARC should be protected against the effects of a lightning strike.

**7.5 Protection of doors.** An audible or visible signal shall operate when any normal entrance-door to the monitoring centre or lobby is not secured. Protective switches installed in accordance with applicable Standard(s) for intruder alarm systems shall be fitted to both doors of the normal entrance in such a way that an alarm condition is created when both doors are opened.

Emergency exit door(s) shall be fitted with a protective switch, which shall create an alarm condition when a door is opened.

**7.6 Emergency entry procedure.** A secure means of emergency entry may be incorporated in the normal entrance only. Whenever such means is incorporated it shall be so designed that a signal is transmitted to another monitoring centre whenever the emergency entry is made.

Where keys are used to allow this, a system shall be designed to ensure such keys are available only to the nominated person(s) within the organisation and are secured in a manner that does not compromise the security of the MARC.

**7.7 Deliberately-operated devices.** Deliberately-operated devices installed in accordance with the applicable Standard(s) for intruder alarm systems shall be provided inside the monitoring centre in positions adjacent to the normal entrance, emergency exit(s) and the normal operating area of monitoring centre personnel.

**7.8 Signalling from the electronic protection systems.** The control equipment shall be such that an alarm condition generated by the electronic protection system is transmitted automatically to another monitoring centre complying with this Standard or to the Law Enforcements Agencies (LEA). Transmission of such an alarm condition shall be by two separate transmission paths NOT using the same physical infrastructure.

**7.9 Closed-circuit television surveillance.** The monitoring centre shall be equipped with closed-circuit television surveillance equipment to include cameras mounted to view each of the following locations separately

- External main entrance to that area of the building occupied by the company.
- Outside the outer normal entrance door to the MARC
- Outside the emergency exit from the MARC.

The monitor(s) provided for viewing the areas specified above, together with any associated switching or multiplexing equipment shall be located in the monitoring centre and under the control of the monitoring centre staff in such a way as to ensure that they have unimpaired ability to view these areas at all times. Adequate illumination of all areas required viewing shall be provided.

A suitable type of image recording system shall be incorporated in order to record all movement at these points.

## **8. COMMUNICATION FACILITIES**

The following communication facilities shall be provided:

**8.1** Voice communication to and across the normal entrance lobby.

**8.2** Equipment within the monitoring centre such that the audio components of all voice telephone traffic concerned with alarm handling and dispatch are automatically recorded. Such recordings shall not be destroyed within 3 months of the event to which they refer.

## **9 RECEPTION OF SIGNALS**

**9.1 General requirements.** The nature of each signal received and its location shall be separately identifiable at the monitoring centre and all signals shall be recorded automatically, giving at least the following information:

- Client/user identification
- Nature of signal
- Date and time of receipt of signal.

**9.2 Operator actions.** In addition, where operator action results from the receipt of a signal, then the details of actions taken shall be recorded, including the date and time of completion and the identity of the person/persons that have performed those actions.

**9.3 Messages.** Magnetic tape messages or electronically generated voice messages shall not be used for the transmission of signals to monitoring centres from intruder alarm systems' automatic dialling units requiring LEA attendance.

## **10. POWER SUPPLIES**

**10.1 Mains power supply.** The public supply mains shall be used as the main source of electrical power for the monitoring centre. The power supplies to (1) alarm signal receiving equipment, (2) the audible warning equipment and (3) the electronic protection equipment shall be protected by fused or circuit breakers within the monitoring centre separately from all other supplies.

**10.2 Stand-by power supply.** Facilities shall be provided within the monitoring centre so that, in the event of an interruption in the public supply, a changeover to a stand-by supply shall be affected automatically.

The stand-by supply shall include a rechargeable battery, located within the monitoring centre, of sufficient capacity for the operation of the alarm signal receiving equipment, together with the electronic protection and the required closed-circuit television systems for a period of not less than 24 hours, or not less than 4 hours where a single stand-by generator is installed or 30 minutes where a second generator is provided. For computer-equipped monitoring centres, as required to support such computer systems, the rechargeable battery shall operate through an uninterruptible power supply (UPS) system.

The ampere-hour capacity of the stand-by supply shall be calculated on the basis of the average hourly current drain multiplied by a factor 1.5. Any charging facility shall be sufficient to provide the maximum load requirements and simultaneously to recharge the battery from the fully discharged state to 80% of the required capacity in not more than 24 hours. In the event of such an interruption in the mains power supply, all the equipment essential to the operation of the monitoring centre shall continue to operate without loss of security or degradation of performance to such an extent that the monitoring centre's ability to receive, process and dispatch signals is impaired.

**10.3 Stand-by generator.** Where a stand-by generator is installed, not necessarily in the protected area, it shall be of sufficient capacity to provide stand-by power. There shall be provision for an adequate fuel supply to operate the generator for at least 24 hours. Such generator shall have an independent means for starting automatically.

Batteries required for starting a standby generator should be charged by a means that is independent of the operation of the generator

The stand-by generator shall be properly maintained in accordance with the manufacturer's instructions and housed in a secure environment. There should be an indication in the operations area of the current source of power.

## **11. MANNING AND OPERATING PROCEDURES**

**11.1 Manning.** Monitoring centres shall be continuously manned by a minimum of two operators. Where a MARC is operating in conjunction with a second MARC and in real-time and the operational methods ensure that the effect is the same as a MARC manned by a minimum of two people, then this requirement is met.

**11.2 Screening.** All MARC staff should be screened regardless of their previous employment. As a minimum each individual should be screened for a minimum of 10 years to the commencement of relevant employment or transfer to relevant employment, or back to the date ceasing full-time education, and their employment over the last 10-year period verified with their previous employers.

The MARC should not employ individuals whose career or history indicates that they would be unlikely to resist the opportunity for illicit personal gain, or the possibility of being compromised, or the opportunities for creating any other breach of security, which such employment might offer.

Potential Staff should be warned that employment may be terminated if their screening cannot be verified, that this is not an indication of unsuitability, simply that it has not been possible to obtain the required positive evidence.

**11.3 Training.** There should be a minimum period of training, appropriate to ensure the minimum competency to carry out the specific duties (eg intruder alarm handling, CCTV operation, etc), provided to all operators before operators are allowed to handle alarms without supervision. Further training should be given on specific subjects such as new equipment or changes in operational procedures.

**11.4 Activations from security systems.** Clear guidelines shall be issued on the actions to be taken on receipt of calls from set or partly set intruder alarm systems (see Annex A). The LEA or such other authority as the client requires shall be notified of the receipt of any valid alarm signal from supervised premises at which the intruder alarm system, or part thereof, is armed. All operating procedures in force which relate to the alarm handling function shall comply with the LEA Intruder Alarm Policy where such exists.

**11.5 Pre-arrangement of arming and disarming.** When appropriate, the client shall inform the monitoring centre by secure means of their intention to set and unset the system at prearranged times.

**11.6 Testing.** The following items of monitoring centre equipment shall be checked for normal operation, and the results recorded:

**11.6.1 At intervals not exceeding 24 hours:**

- External communications with the LEA or other authorities
- The internal clock(s) in the alarm signal receiving equipment, together with any other equipment concerned with ensuring that all activity, including operator actions, is accurately dated and timed.

**11.6.2 At intervals not exceeding 7 days:**

- Main and stand-by power supplies, the automatic changeover equipment, emergency lighting and the MARC alarm system
- All lines provided for the receipt of alarm signals together with those provided for incoming and outgoing voice communications to the monitoring centre.

**11.7 Fault procedures/reporting.** Any item of equipment involved in the receipt, display or onward transmission of an alarm signal shall have a standby facility or procedure that can be brought in automatically or by the MARC operator within 1 hour of the fault being known to the operator.

An appropriate contract(s) with a relevant supplier(s) shall be in place, with an agreed emergency response time for the rectification of all faults that may be found during the checks carried out at 11.6.1 and 11.6.2.

**11.8 Access.** Entry to the monitoring centre, except where taking place under the emergency entry procedure in accordance with Clause 7.6, shall be subject to a documented procedure available to all operators. This procedure shall define the method(s) used to identify persons attempting to enter the monitoring centre, and shall require such persons to be positively identified before access is granted. Access to the monitoring centre shall be controlled in all such cases by positive action by an operator. In any event, not more than three persons shall be permitted in the lobby area at one time. Authorized persons known to the operator shall always enter the lobby first. A log of all visitors to the MARC shall be maintained.

**11.9 Health & Safety.** An audible or visible signal shall be generated within the centre at least once every 60 minutes and this signal shall be acknowledged by an operator within one minute. Failure to acknowledge the signal shall generate a signal at another monitoring centre complying with this Code of practice. It shall be permissible for the normal actions of an operator in operating the alarm signal receiving equipment to reset this timer where the equipment installed is capable of doing so.

**11.10 MARCs receiving signals from another MARC.** A MARC shall be monitored by a second MARC and the following are circumstances in which another MARC shall receive alarm signals:

- opening of emergency door
- simultaneous opening of both normal entrance doors to the centre
- personal attack
- fire alarm activation

**11.11 Audit.** The MARC should carry out a full document audit every 6 months to ensure compliance with the Code of Practice.

**11.12 Complaints Procedure.** The MARC should have a clearly defined, published procedure for the receipt and handling of complaints. Clients should be given details of the person to contact if they wish to complain about any aspect of the service.

## **12. DATA AND DATA STORAGE**

Note: Attention is drawn to the European Data Protection Act

### **12.1 Clients Data**

The data for each alarm system connected to the MARC should be available to operators. The data may be written or stored in electronic memory in which case print outs should be available. The data should include:

- Name, address and telephone contact number(s) of client
- Premises reference number and any special arrangements
- Name, address and telephone(s) numbers of users
- Actions to be taken when an alarm occurs – when to contact the LEA, etc
- Agreed setting and unsetting times where appropriate.

### **12.2 Data communications**

All communications with the MARC shall be recorded and the data shall be maintained for a minimum of the periods stated:

- 3 Months - All telephone communications to and from the MARC with their date and time stamped and capable of being replayed.
- 12 Months - All data communications to and from a MARC relating to monitored events with their date and time stamp.
- 12 Months - The timeframe for the storage of telephone or data communications relating to incidents shall comply with LEA requirements.

### **12.3 Security**

All data should be stored securely, in a fire proofed area and backup procedures instituted for electronic stored data.

### **12.4 Disposal**

All data of a confidential nature should be disposed of in a secure manner.

### **12.5 Logs**

The Marc should keep a log recording all the routine testing, maintenance and emergency servicing to MARC equipment.

### **13 Alarm Handling**

MARC's shall apply procedures that measure the veracity of all alarm signals received prior to passing signals to the LEA, except those that are associated with transmission faults, deliberate operated alarm signals or any signal that are not to be passed to the LEA as agreed in writing with the client.

(Note: The aim of alarm handling procedures is, wherever possible, to ensure that only genuine alarm signals are passed to the LEA. False alarm signals waste LEA resources, affect client insurance premiums and have a negative affect on the security industry. It is up to all parties within the security supply chain, including the client/user, to reduce the number of false alarms passed to the LEA.)

The MARC shall carry out alarm handling measures in accordance with Annex A.

### **14 Emergency Planning**

In the event of a MARC being put out of action there should be an emergency plan for dealing with this situation. The emergency plan should deal with any reasonable abnormal occurrence at the MARC. This will include any problem at the MARC, which causes a degradation of service. The emergency plan should cover technical and other situations. The emergency plan should include:

- a) a means of informing the emergency services
- b) a means of manning backup MARC, and or redirection of signals
- c) a means of informing users of systems affected
- d) a means of informing clients/users

#### **14.1 Hazards**

The emergency plan should take account of possible hazards that may occur. Some of these are listed below:

- a) Complete failure of the MARC processing capability
- b) Faults or damage to utilities
- c) Fire, including exposure to fire in adjoining premises
- d) Flood, or burst water pipes.
- e) Failure of communications infrastructure
- f) Vehicle impact, including rail vehicles and aircraft
- g) Malicious damage
- h) Criminal attack, bomb threats or duress situations
- i) Abnormal activity or staff shortages

#### **14.2 Emergency response**

Emergency response procedures should be developed with local contractors and emergency services to enable the MARC monitoring function to be maintained whilst the emergency incident is investigated, damage contained or repaired.

#### **14.3 Staff procedures**

It is the MARC managers' responsibility to ensure all staff are fully aware of all the procedures to be taken in the event of an emergency. All staff are to be instructed in the location and use of emergency equipment.

A detailed action plan should be provided covering partial evacuation of non-essential staff and the procedures to take if a full evacuation is to take place. The plan should also include procedures for re-entry and or recovery following an incident.

All MARC personnel should receive the necessary training in the emergency procedures at intervals not exceeding 6 months.

#### **14.4 Records**

Records of the action taken during the rehearsal should be kept as part of the normal activity log.

# Annex A

## ALARM HANDLING

### A1 Alarm Processing

(Note: For verified alarm conditions alarm processing may or may not apply)

Following receipt of an alarm signal, and as an opportunity for the alarm to be cancelled by an authorized user, the MARC will allow a delay of not more than 120 seconds before notifying the LEA.

Alarm signals received from deliberately operated devices are exempt from alarm processing.

During the alarm processing delay, the MARC may attempt to contact the user at the supervised premises and/or receive telephone calls from the user in order to ascertain the cause of the alarm condition and designate it as real or false.

When the user cancels the alarm condition during the alarm filtering delay using his authorized pass code, the alarm may be also designated as false.

### A.2 Time parameters for Alarm Processing

(Note: For verified alarm conditions the verified alarm time parameters apply)

The MARC should take action to establish communications with the appropriate emergency service, or commence processing, within the following times of receiving an alarm signal:

- a) for deliberately operated alarms: 30 s for 80% of signals received and 60 s for 98.5% of signals received;
- b) for all other alarms 90 s for 80% of signals received and 180 s for 98.5% of signals received

### A.3 Transmission fault handling

If the MARC receives a transmission fault or transmission interruption it should be handled in one of the following ways:

- a. The MARC operator should endeavour to contact the protected premises and/or user to establish the cause.
- b. If the transmission fault has been sustained for more than 90 seconds then the MARC should carry out its contractual agreement .

## **A.4 Verified Alarms**

(The processing of verified alarms shall be agreed by written contract)

A verified alarm is an alarm condition where an unauthorized entry or attempted unauthorized entry upon the supervised premises, as detected by an I&HAS and transmitted to the MARC, has been verified by one of the following methods and it is considered that a genuine intrusion or genuine attempted intrusion has occurred:

### **4.1 Sequentially verified**

For an alarm condition to be regarded as sequentially verified:

#### **a) Scenario I**

The combined effect of two separate alarm signals arriving at the MARC from the same supervised premises

Following receipt at the MARC of alarm signal, A, (emanating from detector or processor AA), a second alarm signal, B, (emanating from a different detector or processor BB) is received within a specified time interval from the same supervised premises.

If the MARC has been advised by the alarm company that alarm signals from these two sources, AA and BB, provide evidence of a sequentially verified alarm condition, then the MARC should designate the combination of the two alarm signals A and B as representing a verified alarm condition.

If the second alarm signal is not received within the contracted verification time limit, the MARC operator will designate the alarm condition as false. The user may be contacted, but the LEA will not be informed at this stage.

#### **b) Scenario II**

Where only one alarm signal sent by the supervised premises to the MARC is identifiable as representing a sequentially verified alarm condition (The supervised premises CIE has received two separate and independent alarm conditions from the I&HAS and has combined these to send the MARC the sequentially verified alarm signal)

If the MARC receives an alarm signal, C, which is identifiable by the MARC as reporting that a sequentially-confirmed alarm condition exists at the protected premises, then the MARC should regard the alarm signal C as being a sequentially-confirmed alarm signal.

#### **c) Scenario III**

Transmission faults (originating from I&HAS with more than one signalling path) and fault conditions may be handled as first signal, A in Scenario I, in the sequential verification process.

## **4.2 Visually verified**

For an alarm condition to be regarded as visually verified the MARC operator must carry out one of the following for a minimum of 30 seconds if there is no prior evidence, but within the time parameters specified in Section A2:

- a) The operator at the MARC should view images transmitted from the supervised premises directly and in real time; and/or
- b) Images should be recorded by recording equipment within the MARC and the operator at the MARC should review the recorded image(s); and/or
- c) Images should be recorded by recording equipment within the CIE at the supervised premises and the operator at the MARC should review the recorded image(s).

As soon as the operator at the MARC reaches a decision, acting within agreed procedures, that the images emanating from the supervised premises are such as to confirm a genuine intrusion or genuine attempted intrusion within the supervised premises, the alarm signal should be designated as being a visually-verified alarm signal.

## **4.3 Audibly verified**

For an alarm condition to be regarded as audibly verified at the MARC one or more microphones shall have been activated at the supervised premises and the listen-in period stated below must be for a minimum of 30 seconds or prior evidence:

- a) The MARC operator should listen-in to sounds transmitted from the supervised premises directly and in real time; and/or
- b) The sounds should be recorded by recording equipment within the MARC and the operator at the MARC should listen-in to a playback of the recorded sounds; and/or
- c) The sounds should be recorded by recording equipment within the CIE at the supervised premises and the operator at the MARC should listen-in to a playback of the recorded sounds.

As soon as the MARC operator reaches a decision, acting within agreed procedures, that the sounds emanating from the supervised premises are such that they confirm activity within the supervised premises, the alarm signal should be designated as being an audibly-verified alarm signal.

#### **4.4 Client/user verified**

For an alarm condition to be regarded as subscriber/user verified, the MARC will require the subscriber/user verification to be provided by a duly authorised subscriber/user, or the subscriber/user security guards (alarm response/intervention), in which case the MARC may contact only the subscriber/user/security guard in charge of the supervised premises, who will ascertain the cause of the alarm condition and designate it as real or false

Clients are to provide the MARC with at least two names of contact persons who have the ability to respond and will respond to the supervised premises, typically within 30 minutes of receiving a call from the MARC, with keys (key-holders), and have the ability to disarm the alarm system.