IPCRes **guidance**

InFiReS
Insurers' Fire Research Strategy funding scheme

Electronic security systems: Guidance on keyholder selection and duties

Fire Protection Association
Protecting people, property, business and the environment

London Road
Moreton in Marsh
Gloucestershire GL56 0RH

Insurers' Property Crime Research (IPCRes) working group

This guidance document has been developed by the IPCRes working group of InFiReS (see below). IPCRes publications continue the tradition of providing authoritative guidance on crime prevention topics which was established by the Crime Panel of the Association of British Insurers.

First published by

The Fire Protection Association

London Road

Moreton in Marsh

Gloucestershire GL56 0RH

Tel: +44 (0)1608 812 500 Fax: +44 (0)1608 812 501

E-mail: sales@thefpa.co.uk Website: www.thefpa.co.uk

 ISBN 1-902790 48-0

Copies of this document may be obtained from the publications department of the FPA, at the above address, or by calling +44 (0)1608 812 500 or e-mailing *sales@thefpa.co.uk.*

Printed in Great Britain by Modern Colour Solutions. 2.0/07.07

Contents

1. Purpose and scope

The purpose of this guide is to assist owners of electronic security systems at commercial premises in selecting appropriate persons to act as premises keyholders. Keyholders are those persons nominated to operate the system and/or attend and take appropriate action after a security system activation/fault. This publication also provides guidance on ensuring the safety of keyholders, and keyholders' responsibilities when operating the system or attending the site in response to an activation/fault.

There are diverse requirements to be considered, some of which are mandatory in order to comply with legislation, public policies or insurance policy requirements. Electronic security systems owners and operators need to be aware of these requirements and the other recommendations outlined within this document.

Relevant legislation and public policies include health and safety legislation, local authority requirements, and the security system policies of the Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS).

Since the guidance in this document is broadly based, it is recommended that at all stages, the alarm system owner or operator checks with their system installer, insurance provider, local police and local authority for any special requirements concerning the type of alarm system, its operation (or limits on operation) and the nature of any response expected.

The most common type of electronic security system is an intruder alarm, but other systems exist, such as closed circuit television (CCTV) and access control. While this document refers only to intruder alarms, much of its advice will be of general application to other forms of electronic security system.

While addressed to alarm owners at commercial premises, some of the information and advice within this document will be of interest and application to alarm operators at domestic premises.

2. Mandatory alarm and keyholder requirements

Requirements are placed on alarm owners, users and keyholders by legislation, the police and insurers. At all times it is advisable to check whether there are any specific variations to the general information offered in this section, by seeking advice from the relevant organisation.

2.1 Legal requirements

Legal requirements principally cover two areas:

- noise nuisance from audible alarm systems;
- employers' duties to staff keyholders.

Noise nuisance from audible alarm systems

Local authorities have various statutory powers available to them to control the potential nuisance from intruder alarms, such as the repeat or continuous operation of alarm bells/sirens. These powers are set out in the following pieces of legislation:

- The Control of Pollution Act 1974

  Under this Act, the Secretary of State has powers to prepare and approve Codes of Practice giving guidance on noise minimisation. One resulting Code of Practice is targeted at audible alarm systems:

  - Code of Practice on Noise from Audible Intruder Alarms 1982

    This statutory Code of Practice covers the issues of noise/nuisance and notification of keyholder details and response. The Code of Practice also encourages local authorities to use their powers under Section 58 of the Control of Pollution Act to require the fitting of automatic alarm cut-off devices in certain circumstances.

- The Environmental Protection Act 1990

  This places a duty upon local authorities to deal with complaints arising from statutory nuisance, including noise emitted from premises. The local authority must investigate the complaint, and, if it is satisfied that a nuisance exists, it must issue an abatement notice.

  In addition, anyone who is aggrieved by noise nuisance (such as a continuously sounding alarm) may apply to the Magistrates Court for an abatement order. If it seems to the Court that neither the owner nor the occupier can be found, the Court may instruct the local authority to take action itself to curtail the nuisance, and this may well involve forcing an entry to the premises. While there is a duty to re-secure the premises, it is doubtful whether this implies fully resetting the alarm, even supposing the local authority had the means to do so.

  It is a specific defence to a charge of noise nuisance for the business to show that it has complied with the *Code of Practice on Noise from Audible Intruder Alarms 1982,* particularly through the introduction of a 20-minute cut-off. It is anticipated that such a cut-off would, in practice, also be an acceptable defence against local authority action in connection with private residences.

- Noise Act 1996

  This act is concerned with night-time (11pm to 7am) noise from a dwelling/licensed premises, such as noise from an intruder alarm system. Following the service of a warning notice, the person responsible may be liable to a fixed penalty or summary prosecution. If necessary, elements of the alarm system, in particular its sounder, may be removed and seized by a local authority officer acting under a warrant.

- Clean Neighbourhoods and Environment Act 2005

  This is the latest legislation covering noise from audible intruder alarms. Under this Act, a local authority may create designated 'alarm notification areas'. These are areas in which the occupiers/owners of premises with audible alarm systems must nominate keyholders and notify the local authority of the keyholders' contact details.

  The Act also empowers the local authority to enter problem premises, with force if necessary, and, once a warrant has been obtained, to deactivate a system that is causing a noise nuisance. These powers apply to any area, not just designated alarm notification areas. An authorised officer can take whatever steps are necessary to silence the alarm. This might include, for example, disabling the external sounder. Again, the officer is not required to reset the alarm (even if he/she has the means to do so).

Further advice may be obtained from the alarm installer or the local authority environmental health department.

> *Failure to comply with legal requirements may lead to enforcement action and/or prosecution.*

Employers' duties

Many employers require/ask nominated employees to act as premises keyholders and attend the premises should their intruder alarm activate.

The Health and Safety at Work etc Act 1974 and the Management of Health and Safety at Work Regulations 1999 place a statutory duty on employers to safeguard, so far as is reasonably practicable, the health, safety and welfare of their employees. This legislation requires an employer to undertake risk assessments and then carry out effective planning, organisation, control, monitoring and review of the preventive and protective measures employed. An employee acting as a keyholder is doing so as part of their work, so risk assessments should include these duties.

Recorded instances of keyholders being injured during their duties are few and far between, but that does not mean the risk can be ignored. Indeed, according to the type of premises involved or the area in which it is located, the risk of injury may be envisaged as sufficiently serious to suggest the need for a professional keyholding and response company to be used rather than employees. Further practical advice can be found in section 4 below.

There may also be a duty of care owed by an employer to any visitors to the premises, such as an engineer or representative of the alarm installation company, responding police officers or professional keyholders, or even trespassers, by virtue of the Occupiers Liability Acts 1957 and 1984.

Failure to adequately address legal duties may lead to claims for compensation and/or prosecution.

2.2 Police requirements

Police response to intruder alarms is governed by the security systems policies of the Association of Chief Police Officers (ACPO), or the Association of Chief Police Officers in Scotland (ACPOS), as adopted by each local police force. These are entitled *ACPO Policy on Police Response to Security Systems* and *ACPOS Security Systems Policy*, respectively.

One of the requirements of the police policies is that the installing company shall ensure that details of the names, addresses and telephone numbers of at least two keyholders are provided to the alarm receiving centre (ARC). Some police forces also require these details to be supplied to the police force itself. This must be done when:

- installing a new system;
- taking over an existing system;
- a change of keyholder(s) takes place.

To comply with police policies the keyholders must:

- be trained to operate the alarm;
- be contactable by telephone;
- have adequate means of transport to attend the premises at all hours;
- be capable of attending within 20 minutes of being notified;
- have access to all relevant parts of the alarm-protected premises.

Alternatively, details of a commercial keyholding and response service may be provided, subject to it being:

- available at all times via a 24/7 central control room;
- within 20 minutes travel time of the alarm-protected premises.

Failure to comply with police requirements may lead to withdrawal of police response to alarm calls.

2.3 Insurance requirements

After assessing the risk, insurers may impose specific conditions in relation to the use of and response to an intruder alarm. Alarm users should check the exact details with their insurer, but in general terms, a typical insurance policy condition may require that:

- the insured shall appoint at least two keyholders and lodge written details (which must be kept up-to-date) with the alarm company and (if they so require) with the police;
- the keyholders must be available at all times to accept notification of alarm activations, attend promptly and allow access to the premises;

- in the event of notification of any activation of the intruder alarm system, or interruption of the means of monitored communication during any period that the intruder alarm system is set, a keyholder shall attend as soon as reasonably possible. The keyholder shall not leave the premises unattended until the intruder alarm system is set in its entirety, with the means of communication used to transmit alarm signals in full operation.

Any problems in meeting an insurer's requirements should be discussed with the insurer and any alternative agreements recorded in writing.

Failure to comply with an insurer's alarm and keyholder requirements may jeopardise insurance cover.

3. Criteria for appointing keyholders

Keyholders have an important duty to perform and their selection is a matter of considerable responsibility. Keyholders are usually either the alarm operator, employees, friends or neighbours (termed 'non-commercial response'), or a keyholding company (termed 'commercial response'). Whoever is appointed, it is vital that the alarm company be immediately notified of any changes to keyholders and/or contact details. Additionally, where a security system is eligible for police response, the police criteria for keyholders must be met (see section 1).

In choosing keyholders there are certain factors that need to be considered, as outlined below.

3.1 Non-commercial response

Keyholders should:

- be willing and able to undertake the task responsibly;
- be adequate in number (ideally at least four should be appointed);
- be chosen for their proximity to the premises, ideally within a maximum travel time of 20 minutes;
- be able to access all parts of the alarm-protected premises;
- be appropriately trained in all of the processes and procedures for:
  - opening and closing the premises;
  - setting and unsetting the security system;
  - aborting false alarm calls;
  - using any codes necessary for the system and for communicating with the ARC;
- possess/be provided with mobile telephones to allow them to contact:
  - other keyholders;
  - the ARC;
  - the alarm company;
  - other senior personnel, eg to authorise repairs;
  - the police station local to the premises;
  - emergency tradesmen, such as glaziers and builders.

  Telephone numbers for each of the above should be programmed into the memories of keyholders' mobile telephones.

Within the alarm system owner/operator's processes and procedures there must also be provision for keyholder absences, for example due to sickness and holidays.

3.2 Commercial keyholding and response

Various companies offer to hold premises keys and/or attend alarm activations for a fee. These services have become more widespread in recent years, with market demand driven by hardening police attitudes to attending false alarms and increased employer concerns for the health and safety of employees.

Commercial keyholding companies are usually engaged to attend alongside, or instead of, other nominated keyholders such as employees, but may also be engaged to act instead of the police as the 'first response'.

Where such companies attend and find nothing untoward, they will usually re-secure and alarm the premises. If the premises cannot be re-secured and/or the alarm cannot be reset in its entirety, arrangements must be in place for the commercial keyholding and response company to contact other nominated keyholders/representatives of the alarm owner/operator, who must then attend and take appropriate remedial action in accordance with any insurer requirements.

Where commercial keyholding services are sought, alarm owners/operators should:

- consult with their insurers;
- ensure that the prospective service supplier complies in full with:
  - BS 7984: 2001: *Keyholding and response services. Code of practice,* which gives recommendations for the management, staffing and operation of organisations providing such services on a contractual basis;
  - the Security Industry Authority licensing regulations in relation to keyholding and response services (as from 20 March 2006 in England and Wales, 1 November 2007 in Scotland and a date yet to be announced in Northern Ireland);
  - the ACPO/ACPOS security system policies' requirements for keyholders (as appropriate);
- provide the commercial keyholding and response company with a separate identifiable alarm user code (once the company's services have been employed).

The most reliable means of ensuring that a commercial keyholding and response company complies with the above criteria is to choose a company which is approved for keyholding and alarm response services by the National Security Inspectorate (NSI) under their Guarding Gold or Guarding Silver approval schemes.

It is important to ensure that where the alarm is eligible for police response, the appointed commercial keyholding and response company can comply with the police requirement for attendance within 20 minutes, as failure to do so can result in withdrawal of police response.

Prior to the commissioning of the alarm system, details of the commercial response company will need to be forwarded to the alarm company. The alarm company will forward these details to the ARC and, where necessary, the local police.

It is important that the use of a commercial response service should be referred to the relevant insurer for approval. In particular, if, in addition to keyholding services, use of a commercial service is being considered as the first response to signals from the alarm system (ie to take the place of any police response for which the system may or may not be eligible), it is vital that insurance approval is obtained, otherwise the insurance protection may not operate in the event of a claim.

Failure to comply with an insurer's keyholder and/or alarm system response requirements may jeopardise insurance cover.

4. Managing the system

4.1 Control of false alarms

False alarms can be a major nuisance and lead those expected to respond to alarm activations to lose confidence in the alarm system. A well-designed system, properly installed and managed, should function without false alarms, but unwanted activations are often the result of factors that were not recognised and addressed at the time of system design (system issues) or problems when setting/unsetting the alarm (user issues).

If the system causes unwanted activations which exceed the thresholds laid down in the local police force security systems policy, the police may downgrade or withdraw response. Alarm operators who receive a letter warning that police response may be, or has been, downgraded or withdrawn must inform their insurers immediately.

Prompt attention to cure any problem will help prevent further false alarms and may prevent police response being withdrawn. It should be noted that most police forces have, since October 2001, insisted that all new intruder alarm systems, or those seeking restoration of police response after its withdrawal, must have a confirmation capability if they are to be eligible for police response. In such cases, the first activation of the alarm must be supported by the activation of a second detection device or some additional corroborative evidence if the police are to attend. Therefore, if the system is currently unable to provide confirmed activations, vigorous control of false alarms will avoid the cost and inconvenience of a subsequent requirement to convert it to a confirmation system, in order to have response restored.

Anyone able to set or unset an alarm system must be comprehensively trained and totally competent in its operation. Only trained alarm users should have keys to the premises.

> *Failure to inform insurers of downgraded or withdrawn police response may jeopardise insurance cover.*

4.2 Codes

Any codes used in connection with the alarm system should not be available to anyone other than the user. Where a key-pad type of control is used, care must be taken to ensure that others cannot see the command digits being entered. The use of individual (as opposed to shared) codes by alarm users allows those who create problems to be identified and retrained. Failure to exercise reasonable care and caution with regard to code secrecy may jeopardise insurance cover.

4.3 Securing the premises

The keyholder must, before leaving the premises, ensure that the premises are physically secure, that the alarm is set and that any signalling system faults are rectified, unless some other responsible person remains on the premises.

Checklist for keyholders when leaving the premises

Prior to setting the alarm system, keyholders should ensure that:

- all doors and windows are closed and securely locked (this is the most important check);
- there are no staff, contractors, customers or visitors remaining in the premises (apart from any staff who may be acting as escorts to the keyholder – see section 4);
- there is nothing in an area covered by movement detectors which is likely to cause false alarms, for example, swinging signs or badly stacked stock which may fall over;
- there is nothing that may limit the area normally covered by the detector, for example, stock stored in front of the detector;
- the keyholder is ready to leave as soon as the setting procedure is initiated.

If keyholders do not fully set the alarm in accordance with the insurer's requirements and intruders then break in, any subsequent insurance claim may not be paid.

If the alarm cannot be set in its entirety (including all means of signalling), the alarm company must be called. The premises should not be left unattended until the fault has been put right and the alarm has been set correctly and fully.

4.4 Abort process

Many systems have an abort procedure, enabling the keyholder to immediately notify the ARC that a transmitted alarm signal was in fact a false alarm, particularly if this occurs during opening up or closing routines. In most cases, by unsetting the system in the normal manner, automatic abort of police response will be achieved if the unset is completed within 120 seconds. For some systems, it may be necessary to telephone the alarm receiving centre in order to abort a false alarm call, and in such cases a telephone should therefore be made available close to the setting/unsetting equipment.

4.5 Testing and maintenance

Most alarm systems allow the alarm owner or user to test certain functions periodically. For example, most movement detectors contain test indicator lights, enabling alarm users to 'walk-test' the devices to ensure that they are providing adequate coverage. Testing in this manner at frequent intervals is important to ensure that movement detectors have not been masked or sabotaged, and are not in a faulty condition.

The alarm owner should ensure that such tests are carried out at recommended intervals and that any problems identified are reported to the alarm company without delay.

The alarm company is also responsible for making regular inspections of the alarm system, but the alarm owner or operator should make sure that a maintenance contract providing for this is in force and that the inspections are duly carried out and recorded in the maintenance logbook. Such a maintenance contract is normally a condition of insurance provision.

Visits by the alarm company should only be made by appointment, as it is important to ensure that any person wishing to work on the system is properly authorised to do so. The credentials of the visiting engineer should be checked with the alarm company using their established telephone numbers rather than any number supplied by the visitor.

4.6 Action following an alarm activation

If the alarm activates, an appointed keyholder must attend the premises without delay. If the circumstances giving rise to the activation do not allow the ARC to permit the system to be reset without the attendance of an alarm company engineer (in accordance with prevailing conditions specified in relevant British Standards Institution and/or police documents), then the keyholder must remain on the premises until the engineer has attended and re-enabled the control equipment, allowing the alarm system to be reset in its entirety.

Whether or not the activation was caused by an actual break-in, the keyholder must, before leaving the premises, ensure that the premises are physically secure, that the alarm has been reset and that any signalling system faults have been rectified, unless some other responsible person remains on the premises. If damage to the premises and/or the alarm system prevents compliance with any of these conditions, the premises must not be left unattended until the damage has been repaired and the alarm and signalling system has been fully reinstated.

All incidents must be fully recorded in the alarm record book.

4.7 Responding to alarm signalling path faults

A fault on the telephone line or other signalling path connected to the alarm system may prevent the alarm message from reaching its destination. It is important to appreciate that any such 'fault' may have been caused deliberately by someone planning to break in.

In the event of notification of a fault in the system from the ARC, police, telephone company, or the system itself (for example, a warning light or message on the alarm control panel or other device), remedial action must be taken at once. Arrangements should be made for a responsible person to remain on the premises until the fault is rectified. Insurance cover may be jeopardised if the premises are left unattended with any signalling path in a faulty condition. This could be the case whether or not one or more other signalling paths are thought to be unaffected.

To minimise the downtime of a faulty telephone link, alarm owners should subscribe to an enhanced corrective maintenance service where available. This will reduce the amount of time that the premises would have to be occupied in the event of a communications fault. Details will be available from the telecommunications provider.

5. Safety of keyholders attending the premises

As mentioned in section 1, employers have a duty of care to an employee acting as a keyholder.

The most effective means of providing for the safety of the keyholder is to follow systematic and structured processes of risk identification, assessment, training, management and monitoring. Resulting safety measures can be written into a clear policy and procedure to be followed by the keyholder when attending to the alarm system either under normal circumstances (that is, opening and closing of the premises) or in the event of unexpected activations. The following situations should be considered when conducting the assessment and management audit of the risks for the keyholder:

- opening up the premises at the start of working hours, and locking them up at the end of normal working hours. At these times, there may only be a limited number of staff on the premises;
- carrying keys to or from the premises. In some circumstances there may even be risks posed by the keys being at the keyholders' private residences;
- the keyholder receiving a bogus callout message from criminals who are impersonating the police or the ARC;
- responding to a callout and attending the premises out of normal business hours, possibly without the police in attendance.

In order to consider the appropriate level of protection necessary, employers will need to assess the degree of risk involved in each situation.

It is most important that keyholders understand that they are not required to expose themselves to unreasonable levels of risk. They should always be satisfied that it is safe to enter the premises and, if in any doubt, they should contact the police or other assistance and wait for their arrival before proceeding. Instructions to this effect should be stated in the company health and safety policy and in any instructions to keyholders.

An increased keyholder hold-up risk may be likely in any of the following circumstances:

- where the premises is in an area with a high level of crime;
- where the contents are particularly attractive to criminals, especially where the goods stored in the premises are also highly portable (enabling thieves to steal a valuable haul in a very short time if the keyholders were to be compromised);
- at premises such as banks, building societies and retail stores where there are high values of cash or other valuable property in safes or cash centres.

Risks such as these are referred to as target risks within this guidance document.

The risk may also be increased when responding to an unconfirmed alarm activation from a system with confirmation capability, as police attendance will not have been sought by the ARC.

5.1 Normal opening

It is strongly recommended that, as a matter of routine, the keyholder should meet with a colleague at a place away from the premises so that the two may enter together. Alternatively, the keyholder should wait at the premises for a second person to arrive before entering. Consideration should also be given to implementing a system whereby one person enters, while another employee stands some distance away and waits until he/she receives a pre-arranged 'all-clear' signal before entry.

On arrival at the premises, keyholders (especially if unaccompanied) should observe the premises from a safe distance and be alert for anything suspicious. On approaching the premises, they should make a careful examination of the entrance door and the outside of the property, making sure that everything is in order. If there is evidence of an intruder having been on the premises, the police should be called at once and keyholders should not enter until police have attended. Keyholders should be alert to anyone suspicious waiting near the entrance or in vehicles nearby. If in doubt, they should seek assistance and/or wait until a colleague arrives.

In the case of target risks, it is possible that intruders may already be on the premises (having previously forced an entry) in order to overcome employees as they arrive, one by one. This possibility should always be taken into account. A sensible precaution is to agree a pre-arranged signal to indicate to employees who are not keyholders that the premises are safe.

For target risks, the keyholder and/or escort should be provided with portable personal attack alarms which will operate in the vicinity of the premises, as well as inside them. These alarms should operate silently, triggering the premises' alarm to send a special personal attack message directly to the alarm receiving centre. These types of alarms should preferably be capable of locating and reporting exactly where the member of staff is situated.

Particular care should be taken in respect of the arrival of cleaners outside trading hours. It is recommended that their identification should be verified before allowing entry to the premises.

5.2 Normal closing

Keyholders should preferably not be left in a position where they are on the premises on their own. Where possible, at least one other member of staff should act as an escort and accompany the keyholder at the time the keyholder is closing up the premises and leaving the vicinity with the keys.

If exterior lighting during the hours of darkness does not continuously illuminate the area outside the final door, lighting automatically operated by means of a movement sensor should be fitted to give protection to the keyholder.

Before exiting the premises to operate shutters or grilles, or to complete the final lock up, the keyholder should look around outside the building for anything that appears suspicious. If there is any cause for concern, the police should be contacted.

For target risks, particularly those situated in areas with a high crime rate, it is recommended that a mutual support scheme is arranged so that other local traders who overlook the premises are asked to be vigilant while the premises are being locked up.

Where another employee is acting as an escort to the keyholder, the escort should remain with the keyholder if the keyholder is delayed. For example, if the keyholder's personal vehicle is disabled, the escort should stay with the keyholder, as this may have been done deliberately so that the keyholder is left alone in the vicinity of the premises.

5.3 Monitored opening and closing

Where there is an intruder alarm with remote signalling to an ARC, arrangements can be made with the ARC to monitor the opening and closing of the intruder alarm system. Any attempt to open the premises and unset the alarm system during the agreed closed period would then be regarded as a suspicious event which must be notified to the alarm owner/operator or nominated keyholder. This facility can also be useful where there is a risk that others tasked with setting the alarm may fail to do so (for example contract cleaners), or a risk of keyholders being brought to the premises under duress and forced to open them outside normal business hours. Where this system is in operation, legitimate changes to the usual opening or closing times must be pre-notified to the ARC.

For target risks, the keyholder should be supplied by the alarm company with a special codeword to be used if they are forced to open up the premises under duress. This special codeword would indicate to the ARC that the keyholder is being made to open up the premises by criminals.

Some alarm system control panels allow the keyholder to send a 'duress code' signal (for example, by entering a certain sequence of characters on a keypad). This sends a unique and dedicated signal to the ARC, indicating that a duress situation exists at the premises. It is worth noting that most police forces are thought to follow the *Ten Point Plan for Personal Attack Devices* contained in Appendix T of the *ACPO Policy on Police Response to Security Systems.* Among other provisions, this restricts the use of duress codes for new systems to those systems which meet the requirements of Grade 4 of BS EN 50131: *Alarm systems. Intrusion systems.*

Note: Kidnap and duress. The kidnap or duress of a keyholder (or other potential target) is not common. However, the risk should be addressed, particularly in the case of target risk premises.

Where a kidnap or duress situation is a possibility, the employer should have in place a system to address kidnap/duress situations, should they occur. If no system exists, one should be established, in consultation with the local police and with insurers.

5.4 Personal attack and duress codes

Where personal attack alarms are provided, these should operate silently without a bell or other audible warning being sounded on the premises which might cause any criminals to act violently.

Where the ARC receives an alarm from a personal attack device or receives a coded message which indicates duress, it will notify the police using a special message format which alerts them to the fact that a hold-up is in progress or that someone on the premises is under criminal duress. The *Ten Point Plan* urges filtering of personal attack calls prior to their being passed to the police for response. This means that additional information would have to be supplied – obtained, for example, by telephoning the premises – before the police will attend.

5.5 Emergency call-out

If the keyholder receives a call-out message outside normal hours, they should check that it is a genuine message. If the caller says they are from an ARC, the keyholder can confirm this by exchanging codes with the ARC. Alternatively, the keyholder could telephone the ARC to make sure the call was valid before leaving for the premises. The keyholder should telephone the originally recorded number for the ARC and not rely on information given by the caller. If there is any suspicion that the call-out message is bogus, the keyholder should immediately telephone the police and follow their instructions.

If a police response is expected, on arrival at the premises, the keyholder should wait at a safe distance but within sight of the premises until the police arrive. If the police do not arrive within a reasonable time, the keyholder should contact the local police station for advice before approaching the premises. The keyholder should specifically

request the attendance of the police and not enter the premises alone unless satisfied that it is safe to do so. Since not all police stations are open continuously, the keyholder should have the number of the nearest station that is open 24 hours a day.

5.6 Keyholder on premises when the system cannot be reset

If the system cannot be reset following an activation, the keyholder needs to remain on the premises until this can be rectified, unless he/she is relieved by an appropriate person. However, while waiting at the premises the keyholder may be vulnerable, and special procedures must be followed:

- wherever possible, the keyholder should telephone another employee or a member of the management or security staff directly to seek additional support;
- the police should be made aware that the keyholder is on the premises and the reason why, and be asked to inform their local patrol(s);
- the premises should be secured from the inside and tradesmen or others admitted only if the visit has been pre-arranged and they can show appropriate identification.

It may be possible, via neighbourhood watch schemes or by a mutual aid arrangement with other local businesses, for security staff at neighbouring premises to be alerted so that they may keep the premises under observation and give assistance if required.

Assistance may also be obtained from professional security companies who may be able to provide:

- security guards to support or relieve the keyholder;
- visits from patrols;
- regular contact by telephone.

It will be necessary to make contingency arrangements beforehand for such services.

5.7 Mobile telephones

Keyholders must be in possession of mobile telephones. Their batteries should be maintained at a high state of charge so that, for example, a voice call to a colleague may be left open throughout vulnerable operations, such as the opening of a target premises or responding to an alarm activation.

5.8 Cash and valuable property in safes

It is advisable that, where there are safes containing cash or other valuables, the keyholder having charge of the premises keys should not also have the safe keys or be aware of any safe combination number.

If it is necessary for the holder of the premises keys also to hold safe keys, the safe should have a dual locking system, with one person keeping one key (or combination number) and a second person having the other key (or combination number), so that they must both be present before the safe can be opened.

Alternatively, a time lock should be provided, so that even with the appropriate key or combination number, the safe cannot be opened until the pre-set time has been reached. Where a time lock is used, the time set for opening should be after the premises are fully occupied, and not when a keyholder first arrives to open up.

As a deterrent to criminals, special anti-hold-up measures such as time locks and time delay locks (which delay access to the contents of a safe for a predetermined period) should be publicised by an official notice posted on the safe or in the vicinity of it. Staff members should also be informed of these special security measures and be trained how to respond to criminals in the event of a hold-up.

Other IPCRes guidance documents

Other documents developed under the Insurers' Property Crime Research (IPCRes) scheme include:

Intruder alarms and a harmonised European standard

This guidance document reviews the progress that has been made in pursuit of a harmonised European Standard for the design and installation of intruder alarms and offers practical advice for those uncertain about their choice of intruder alarm.

Alarm signalling using the internet protocol: Part 1: An overview

This document is aimed at those seeking an introductory understanding of different methods of transmitting security alarm data over local area network and wide area network infrastructures, using internet-based protocols.

It investigates and reports on internet protocol (IP) signalling designed to be used to transmit intruder, hold-up and other critical signals from a monitored location to an alarm receiving centre.

Alarm signalling using the internet protocol:
Part 2: Considerations for insurers

This document considers the issues for insurers that are emerging with the introduction of alarm signalling technology and proposes a basis for evaluating the various implementations of the technology. It aims to help the insurance industry assess whether IP-based alarm transmission systems are fit for the purpose of forming the signalling link from an alarm system to an alarm receiving centre.

Convenience ATMs: Recommended security measures

This document provides advice on the security of 'stand-alone' or 'freestanding' automated teller machines (ATMs), typically located in convenience stores, petrol stations, supermarkets, pubs, and clubs etc. The guidance given within this document is designed to reduce the risk of crime and therefore insurance losses occurring on premises where such ATMs are installed.

Security fog devices

These guidelines have been produced to assist potential users and specifiers in understanding certain factors that need to be considered before installing a security fog device.

IPCRes guidance

InFiReS
Insurers' Fire Research Strategy funding scheme

Electronic security systems: Guidance on keyholder selection and duties

London Road
Moreton in Marsh
Gloucestershire GL56 0RH

Fire Protection Association
Protecting people, property, business and the environment