



ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS

1. INTRODUCTION

1.1 The Association of Chief Police Officers (ACPO) of England, Wales and Northern Ireland recognise the rapid development of technology and its use within security systems. This policy details the police response, which can be expected to an electronic security system, which is identified in the ACPO "Requirements for Security System Services".

1.2 To enable a security system to be recognised within the ACPO Requirements for Security Services it must comply with the ACPO Policy on Response to Security Systems and a recognised standard or code of practice controlling manufacture, installation, maintenance and operation. Such standards must be in the public domain and not be product based.

1.3 The installation and services provided by the installing company and an alarm receiving centre / monitoring centre, shall be certified by a UKAS accredited certification body in accordance with the provisions of the ACPO Requirements for Security Services.

2. SCOPE OF POLICY

2.1 Type A - Remote Signalling Systems.

Systems terminating at recognised Alarm Receiving Centres (ARCs), Remote Video Response Centres (RVRCs) for CCTV and System Operating Centres for vehicle tracking. All centres must conform to BS 5979 (Cat II).

Unique reference numbers (URNs) will be issued to these systems. In the case of stolen vehicle tracking systems the URN will be issued to operating company or monitoring centre, not to each vehicle.

2.2 Alarm Receiving Centres dealing solely with alarm systems within its own company premises (in-house monitoring), are exempt from the BS5979 Cat II certification provided:

- a) the facility was operational with police consent prior to 31st October, 1995, and there has been no change of premises.
- b) there is no monitoring of any alarm or security device in premises other than those owned by that company, i.e. no 3rd party commercial risk is undertaken.
- c) the intruder alarm systems are operated in accordance with all other aspects of this policy.

2.3 Type B - Security Systems.

Systems, for which police attendance may be requested, and which operate outside the procedures identified at Section 1 and Type A requirements.

Unique reference numbers will not be issued to these systems.

3. POLICE ATTENDANCE

3.1 For **Type A** security systems there are three levels of police intervention.

LEVEL 1 – Immediate/Urgent.

It should be noted that police response is ultimately determined by the nature of demand, priorities and resources which exist at the time a request for police response is received.

LEVEL 2 – Routine.

Police response is desirable but attendance may be delayed, e.g. due to resource availability.

LEVEL 3 – Withdrawn.

No Police attendance, keyholder response only.

3.2 **Type A Systems.**

The police service has adopted a policy on the use of confirmed alarm technology as part of the effort to reduce false calls.

3.3 All new applications will only qualify for a URN and police response if messages to be passed to the police are to be confirmed. Unconfirmed systems, which become subject to withdrawal of police response, will only qualify for restoration of response if messages passed to the police are confirmed.

3.4 Security systems issued with a Unique Reference Number (URN) will receive LEVEL 1 response until two false calls have been received in a rolling 12-month period.

3.5 Following two false calls in 12 months the police response will move to LEVEL 2 and the customer will be advised in writing, with a copy being forwarded to the maintaining alarm company. Following five false calls in 12 months LEVEL 3 will apply and police response will be withdrawn. The occupier will be advised in writing with a copy to the maintaining company, who will be required to instruct the ARC not to pass alarm messages to the police. This will remain valid until the system has been free of false calls for 3 months.

3.6 Following withdrawal of response, police response may be restored following 3 months free of false calls. To restore response, the occupier or the security company shall apply in writing to the Chief Officer of Police, supported by evidence from the security company that the system has been free of false calls, that the original cause has been rectified and the system has been upgraded so that only calls identified as confirmed may be passed to the police. After police response has been resumed only activation's, which have been confirmed, will be passed for police attendance. Should the level of false calls result in the restoration of response being delayed for more than 6 months, the URN will be deleted and the occupier and the security company advised in writing.

3.7 ACPO will invite representatives of relevant organisations to assist in the monitoring of the effect of confirmed technology and to make recommendations to update the policy and/or relevant codes of practice.

3.8 **CCTV Systems**

Requirements for companies installing and monitoring remote CCTV systems.

3.8.1 The police requirements for remotely monitored detector activated CCTV systems to enable such systems to gain Unique Reference Numbers (URN) from police forces. (**Appendix R**)

3.9 **Personal attack alarms (deliberately operated devices).**

A personal attack alarm may be operated to summon urgent police assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that defined area. If the device is portable it will not require any additional information concerning its location, other than the address of the premises. These devices must not be used to summon assistance in circumstances other than this. Misuse to summon police attendance to non-attack incidents may result in Level 3 response.

3.10 In a system with both personal attack (deliberately operated) and security systems, the remote signal shall differentiate between the two types. Unless this distinction is made, any withdrawal of Police response sanction will apply to all p.a. calls from the system.

3.11 Personal attack (p.a.) systems conforming to section 3 will attract LEVEL 1 response. Where the threshold for withdrawal of police response is reached the withdrawal will apply to the facility (intruder or p.a.), which has caused 3 or more of the false calls. That part to which response has not been withdrawn continues to receive response until it reaches the withdrawal threshold in its own right. Police response is then withdrawn, but will count from the original withdrawal date so that application for restoration is contemporaneous for both facilities. Following withdrawal of response to the pa, police response may be restored following receipt of evidence from the security company that the pa has been free from false calls for a 3-month period. Response may be reinstated to PAs before three months free from false calls, if the alarm company can satisfy the police force concerned, that a significant change has been made to that particular system to prevent further false calls. Re-instatement in this way can only be obtained once.

3.12 **Type B Security Systems**

To obtain police attendance, Type B systems will require some additional indication from a person at the scene that an offence is in progress, which indicates that police response, is required. This will require human intervention such as member of public, owner or agent visiting, or viewing the premises and the level of police response will depend on the quality of the information received. The addition of electronic means to provide confirmation will not promote such systems to Type A or achieve police response. Calls for police attendance will be by 999 or public telephone lines as appropriate.

3.13 Automatic dialling equipment must not be programmed to call police telephone numbers. If so programmed, they will not receive a police response.

3.14 Calls received from non-compliant central stations and calls from compliant alarm receiving centres without a valid URN will not receive a police response.

4. LIST OF COMPLIANT COMPANIES INSTALLING TYPE A SECURITY SYSTEMS

4.1 To identify companies conforming to this Policy it is necessary for each Police Force to hold a list of policy compliant companies. Inclusion on the list does not amount to confirmation that the Police have inspected the company or its work. Only companies so listed may install, maintain and/or monitor Type A systems in the particular Police area. Where a company loses police recognition under the policy, its existing customers will have 12 months in which to make alternative maintenance/monitoring arrangements.

Companies applying for inclusion on the above list must do so using **Appendix B** and shall:

- (a) Be inspected and recognised by an independent inspectorate body as at paragraph 1.3.
- (b) Not have as a principal or employ in the surveying, sale, installation or maintenance of security systems, persons with criminal convictions (other than spent convictions). **Appendix C** sets out a procedure for the implementation of this requirement. It is a matter for individual Chief Constables to adopt this procedure and such adoption will be identified at **Appendix A**.

4.2 **Information to Customer**

The compliant list is for police administrative purposes. Members of the public seeking advice from the police about companies capable of installing remote signalling alarms will be advised to seek information from inspectorate bodies directly. (**Appendix H**)

4.3 **Notice to Customer Type A Systems**

Prior to the signing of contract the installing company shall give to the customer a document outlining the Police Policy. (**Appendix I**)

5. NOTICE TO INSTALL TYPE A SECURITY SYSTEM

- 5.1 Notice of intention to install a Type A security system requiring a URN, shall be sent to the Chief Officer of Police in the form of **Appendix F**.

This will result in the issue of a Police Unique Reference Number (URN), which must be quoted in any communication regarding the installation. An activation received from an ARC without a current police URN will be treated as a Type B system and not receive a police response without additional evidence of an offence in progress.

Facilities for inspection of the installation shall be made available if required by the Chief Officer of Police.

5.2 Variations

Any variations to the original URN application details shall be notified within 14 days to the Chief Officer of Police in the form of **Appendix F**.

6. KEYHOLDERS

- 6.1 All premises with Type A systems shall have at least two keyholders, details of whom will be maintained by the ARC or through arrangements with a central keyholding service. Keyholders shall be trained to operate the alarm, be telephone subscribers, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified. The maintenance of keyholders records is the responsibility of the Alarm Receiving Centre, not the police.

- 6.2 Keyholders must comply with the Association of British Insurers Guidance on Keyholders for Commercial Premises.

- 6.3 Failure of keyholders to attend when requested on three occasions in a rolling twelve month period will result in the withdrawal of police response for a three month period.

7. DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

- 7.1 Save for as outlined at 7.2 there is no requirement for security systems to have audible or visual warning devices delayed following activation of the system.

- 7.2 Intrusion detection systems in commercial premises may be required to have audible and visual alarm warning devices delayed for a maximum of 10 minutes where the chief officer of police determines that the call handling time, location of premises and the Force Service Standard would enable officers to attend the premises within that time. (See **Appendix A**)

- 7.3 Occupiers of premises within such a 10 minute delay area may apply to have this requirement waived due to individual circumstances.

8. FALSE ALARM MONITORING

- 8.1 There is an obligation on the part of the installer, maintenance company, customer and the monitoring centre to employ all possible means to filter out false calls. Companies installing Type A systems will have their performance judged on their false call rate. This may be achieved by use of a formula and referral to the installer's inspectorate body as set out at **Appendix D**. The Force may determine whether the formula will be based on police statistics or on those supplied by the company.

- 8.2 Definition – For the purpose of this policy, a false alarm is an alarm call which would normally be passed to the police and has not resulted from:
- a) a criminal attack, or attempts at such, on the protected premises, the alarm equipment or the line carrying the alarm signal.
 - b) actions by the emergency services in the execution of their duty.
 - c) a call emanating from a personal attack system made with good intent.
- Activation of detectors without apparent damage or entry to the premises and line faults will be considered as a false alarm unless proved otherwise.

9. ADMINISTRATIVE CHARGES

- 9.1 Each application for a Unique Reference Number is subject to an administration fee payable by the system user. Forces may determine the charge up to a ceiling of £35.00, inclusive of VAT. The fee is identified at Appendix A and the ceiling will be reviewed by ACPO every two years. The current policy on charging is set out in Appendix E.

10. MEMORANDUM OF UNDERSTANDING

- 10.1 For non-compliance or poor performance by a compliant company or alarm receiving centre, the procedure set out in the Memorandum of Understanding should be implemented before suspension of URNs. (**Appendix J**).

11. MISCELLANEOUS PROVISIONS

11.1 Data Protection Act 1998

Data supplied to the Chief Officer of Police in relation to security systems may be held on a computer and companies should notify clients that (a) limited data supplied by them may be held on Police computers and (b) where the data is relevant to a complaint, it may be disclosed to the relevant independent Inspectorate body recognised by ACPO.

Information supplied must be accurate and kept up to date. Any alterations to the personal data supplied by Alarm Companies must be notified to the Chief Officer of Police within 14 days.

11.2 European Court of Human Rights Considerations

The policy has been drafted taking into account the appropriate principles of the Human Rights Act 1998. It has also been subject to suitable legal vetting.

11.3 Racial Equality

The policy has been drafted taking into account the appropriate principles of Sections 2 (2) and (3) of the Race Relations Act (Statutory Duties) Order 2001.

11.4 Advertising

Companies shall not use terminology which might raise in the mind of the customer a guaranteed or unrealistic expectation of police response to a security system and shall not use an ACPO logo or reference in advertising material without written permission from the ACPO General Secretariat, or a police force logo without the permission of the relevant chief officer of police.

12. FINAL DISCRETION

- 12.1 The policy does not impose any liability on this Force, its officers or employees or the Police Authority arising out of any acts or omissions connected with the security system installation, including failure or timeliness in responding to any activation's. The Chief Officer of Police reserves the right to: -
- (a) refuse to admit a company to the compliant list.
 - (b) refuse to issue a Police URN for any installation.
 - (c) Refuse Police response to any security system installation.
 - (d) To alter, amend or add to this policy as necessary through the ACPO Security Systems Group.
- 12.2 Issues, which may require amendment to this policy, must be forwarded to the Chairman, ACPO Security Systems Group, the address of whom may be obtained from Police Headquarters. The Chairman meets with representatives of the security industry, independent inspectorate bodies, the Association of British Insurers and the British Retail Consortium and other representative organisations to review such matters.
- 12.3 The ACPO Security Systems Policy is the copyright of the Association of Chief Police Officers (ACPO). This Policy is available on the ACPO website at www.acpo.police.uk and www.securedbydesign.com and may be downloaded for individual use.

APPENDIX A

(Example. Remains as at present with force response policy and will include the adoption of options to check convictions and make administrative charges. It must not be used to introduce changes to the principles of the policy.)

Force crest, Chief Officer's name and Headquarters Address

The ACPO unified intruder alarm policy has been adopted by the Police/Constabulary. The following variations permitted under the terms of the policy apply in this police area.

(Examples)

1. Automatic 999 dialling alarm equipment is not permitted.
2. All central monitoring station alarm messages must be transmitted to our Force Control Room, Police Headquarters on dedicated ex-directory telephone lines. The number of which will be disclosed on receipt of a signed policy agreement (Appendix B) ...(details of any annual fee/ premium rate charges).
3. The Police/Constabulary Service Standard is to aim to attend all urgent calls within 10 minutes in the following areas - and town centres. Commercial premises in these areas must have a 10 minute audible sounder delay on remote signalling systems. In all other areas an instant sounder is permitted. In exceptional circumstances companies may apply in writing for exemption to the delay requirement according to individual risks.
4. Commercial alarm companies must enclose a stamped addressed envelope with all correspondence requiring a reply.

All correspondence should be addressed to the Supervisor, Alarm Administration Department,(address).

The Unique Reference Number (URN) must be quoted in all correspondence. In the interests of maintaining security of records all enquiries concerning individual alarm systems must be made in writing. Telephone enquiries regarding systems or particular alarm activations will not be accepted.

POLICY AGREEMENT FORM

APPENDIX B

This form must be signed by an authorised person at the company head office.

I have read the (name of force) Police/Constabulary Security Systems Policy and Requirements for Security Services. I agree to comply with every requirement of these documents.

I acknowledge that failure to comply will result in my company no longer being accepted by the (name of force) Police or being included on the (name of force) Police list of compliant companies.

I am authorised to sign this document on behalf of (name of company).....

My company is inspected byfor the following:.....

Signature.....

Print Full Name

Date.....

Name of Company.....

Position in Company

Address

.....

.....

Post Code

Telephone Number

Fax Number

Email address.....

TO BE RETURNED TO: Alarms Administrator
() Police
Police Headquarters
(Address)

Data Protection Act 1998

Personal data supplied on this form may be held on, and/or verified by reference to information already held on computer

APPENDIX C

DISCLOSURE OF CONVICTIONS

It is suggested that the procedure should only be entered into with companies on the List of Compliant Security System Installers of a Police Force or a company making a bona fide application for admittance to the List.

It is emphasised that the Rehabilitation of Offenders Act 1974 applies, and 'spent' convictions cannot be considered.

The intention is to curtail those with criminal convictions having access to premises and information relating to the security of premises. The offences should therefore be relevant, such as involving theft, dishonesty, serious assault, drugs and offences of indecency.

PROPOSED PROCEDURE

- (i) Police checks must not take the place of normal recruitment procedures. References should be required and taken up in the case of all new appointments, with unexplained gaps in employment being satisfactorily accounted for.
- (ii) Each applicant seeking employment where their duties will include surveying, sales, installation, maintenance and administration of security systems (in accordance with BS7858) with a company on a Force's List of Compliant Intruder Alarm Installers, or a prospective company wishing to go on the List, will be required to complete a form. The form will be consistent with the model layout as shown at Form A. This will be done after selection, but before appointment.
- (iii) Employers may wish to make a statement available to people who may be subject to a criminal records check under these arrangements, to reassure them that ex-offenders will not automatically be rejected. A model statement is offered at Form B.
- (iv) The police should not be asked to confirm criminal records where the person concerned has admitted a conviction which would clearly render him or her unsuitable for employment in the surveying, sales, installation, maintenance and administration of security systems.
- (v) When a police check is required, the employer should then pass the request on to the Chief Constable of the Police Force for their area.
- (vi) Employers must make every effort to confirm the identity of the applicant before the police are required to process the check. They must also confirm the correct spelling of the full name, the date and place of birth and current address.
- (vii) All applicants must give written permission for the police to institute checks and also advise employers where they consider an applicant unsuitable within the terms of the Policy.
- (viii) The police check will be limited to a PNC check against criminal convictions only. The police will reply stating the person is suitable or that these details appear identical with a person who is considered unsuitable. Details of convictions will not be passed on to the employer.
- (ix) Where a person wishes to complain about this decision on the grounds they have been incorrectly identified, they should have an opportunity to make representations to the police. This should be done in the first place through the employer. Where such a complaint is received by the police, the grounds for rejection will be disclosed to the complainant, but not the employer.

APPENDIX C (continued)

- (x) This Policy only applies to new employees of existing companies on the Compliant List and to any prospective company wishing to go on the List. If someone who is working for a company on the Policy Compliant List is subsequently identified as being unsuitable through his/her criminal convictions, police forces may notify the relevant employer. The subject of the report will be informed.

APPENDIX C(continued)

FORM A TO BE RETAINED BY THE POLICE

REQUEST FOR A POLICE CHECK IN RESPECT OF AN APPLICATION FOR EMPLOYMENT AS A SECURITY SYSTEM INSTALLER

PART A - To be completed by the applicant in BLOCK CAPITALS

I am aware that this employment is subject to a police record check and I consent to such a check being performed. This has been explained to me and I understand spent convictions are not considered by the police in assessing my suitability. I authorise the police to inform my employer if they consider me to be an unsuitable employee under their Force Policy on Security Systems, because of any criminal convictions.

Signature Date

Surname/Family Names

All First Names

Maiden/Former Names

Date of Birth / / Place of Birth Sex M/F

Present Address

.....

.....

Previous Addresses in last 5 years (give dates):

.....

.....

.....

(continue overleaf if necessary)

Have you ever been convicted at a Court for any offence, which is not now spent under the terms of the Rehabilitation of Offenders Act 1974. YES/NO

If YES, provide details overleaf, including approximate date, the offence, and the Court or Police Force, which dealt with you.

APPENDIX C (continued)

PART B - To be completed by the employer

The person identified above satisfied the conditions for requesting a police check set out in the ACPO Policy on Security Systems. The particulars provided have been verified and I am satisfied they are accurate.

SIGNEDPRINT NAME.....

POSITION IN COMPANY.....

DATE

NAME AND ADDRESS OF COMPANY.....

.....

PART C - For Police use only

PNC/NIB Records only have been checked against the above details:

●□□□□□□□□□□&

No trace on details supplied.

○□□□□□□□□□□er

●□□□□□□□□□□&

The subject appears identical with the person whose criminal record is attached.

○□□□□□□□□□□er

SIGNED DATE

ALL FORMS TO BE RETURNED TO THE NOMINATED OFFICER IN THE FORCE FOR IMPLEMENTATION OF THIS ACPO SECURITY SYSTEMS POLICY.

THIS FORM AND THE CRIMINAL RECORD MUST BE RETAINED BY THE POLICE

APPENDIX C (continued)

FORM B

DISCLOSURE OF CRIMINAL CONVICTIONS

NOTICE TO:

The Police, in applying their policy on intruder alarms, may preclude a company from its List of Compliant Security Systems Installers if a principal or employee has criminal convictions.

In connection with your employment/application for employment, you are required to supply the personal information. Any convictions, including bind-overs, should be shown. You are required to sign the form authorising the Police to inform your employer if you are considered to be unsuitable for employment under the terms of their Security System Policy.

It should be noted that failure to provide relevant information, or to give false information, could lead to prosecution for an offence under Section 16, Theft Act 1968.

Following the checks the Police, at their discretion, may advise an employer/ prospective employer that an individual is not acceptable because of their convictions but in so doing they will NOT reveal actual details.

Where you believe you have been wrongly identified, you are entitled to make representation to the Police. This should be done through the employer in the first instance.

If there is insufficient space on the form overleaf to fully answer any question, please continue on a separate sheet of paper.

**NB THE REHABILITATION OF OFFENDERS ACT 1974 APPLIES TO THIS
REQUEST FOR INFORMATION. YOU ARE NOT REQUIRED TO DISCLOSE
A CONVICTION, WHICH HAS BECOME SPENT UNDER THE ACT.**

FALSE ALARM MONITORING FORMULA**APPENDIX D**

The following formula may be used to monitor the performance of companies installing remote signalling alarms

$$\text{upper action level} = \left(a + \frac{1}{N} \right) \left\langle 1 - \frac{1}{9(Na + 1)} + Z \sqrt{\frac{1}{9(Na + 1)}} \right\rangle^3$$

- a** = the force false alarm rate for a particular reference period (e.g. 28 days, month or year)
- N**= the number of installations for a particular company
- Z** = the value taken from tables based on normal distribution. The figure of 1.64 has been chosen to give the following producers risk and consumer's risk.

Producer's risk - the probability of wrongly identifying as inefficient a company whose false alarm rate is the same as the force rate is 1 in 8000.

Consumer's risk - the probability of wrongly identifying as efficient a company whose false alarm rate is the same as the upper action level is 7 in 8. This would be less for companies operating above the upper action level.

NB. Each installing company will have a different upper action level dependent upon their total number of installations.

Mode of application

The application of the formula is only a guide, which will intimate to those monitoring performance that a problem may need to be addressed.

Where a company has a false alarm rate which exceeds the upper action level for that particular company for 3 consecutive months or for any 6 months in a rolling 12 month period the following procedure will apply.

The alarm installation / maintenance company will be notified in writing that their false alarm rate exceeds their upper action level. They will be requested to reduce their false alarm rate to inside of their upper action level within 3 months. The companies inspectorate body will also be informed.

- (i) Where a claim is made that the upper action level has been exceeded on the grounds of unique types of alarm installations a revised rate may be introduced at the discretion of the Chief Officer of Police. Where the Chief Officer considers a claim for a revised upper action level is unacceptable he may refer the matter to the appropriate independent inspectorate for arbitration.
- (ii) Where a reduction to the false alarm rate is not achieved within a three month period the Chief Officer will consider the following options-
 - (a) if the company appears to have made little or no effort to resolve the problem an immediate withdrawal of facilities to acquire new unique reference numbers (URNs) will take place until the company has reduced their false alarm rate to within their upper action level. The circumstances will be reported to the appropriate inspectorate body as a serious non-compliance with the ACPO Requirements for Security Systems Services document..
 - or**
 - (b) if the company demonstrates it has tried but been unsuccessful in reducing their false alarm rate to within their upper action level the circumstances will be reported to the appropriate inspectorate body as a non-compliance. The Chief Officer may agree objectives with the company to resolve the matter, in such cases the URN facility will not be withdrawn.

Last revision 04/2004

ADMINISTRATION CHARGES

APPENDIX E

The following charging structure is adopted by all police forces seeking to recover administration costs in respect of security systems. Payment shall be made to the individual police force in accordance with arrangements set out at **Appendix A**.

1. Each application for a Unique Reference Number is subject to an administration fee payable by the system user. Forces may determine the charge up to a ceiling of £35.00, inclusive of VAT. The fee is identified at Appendix A and the ceiling will be reviewed every two years by ACPO.
2. Upon receipt of the administration fee, a URN will be allocated to the system and issued to the maintaining company. If the applicant's cheque fails to clear, the URN will be cancelled and the alarm company informed.
3. The administration fee is payable for:
 - a) New URN applications
 - b) New occupiers of premises taking over existing security systems (false alarm history deleted)
 - c) Applications for re-issue of deleted URNs
 - d) Existing user changing alarm company (system retains false alarm history unless upgraded to confirmed)

Where a security company takes over another security company, or a premises changes name only, no charge is made and the systems retain their false alarm history.

NB. Security company taking over another security company. Where a security system has been cancelled by a security company (company A), prior to notification being received that the security system is to be taken over by another security company (company B), the system will be regarded as a new security system.

4. In the event the installation does not proceed after the URN has been allocated, the fee is non-returnable.
5. All security system monitoring centres operating under this policy must utilise the dedicated ex-directory lines nominated by each police force. An access fee may be chargeable and will be recovered by either a) the use of premium rate telephone call charges or b) an annual fee. The method chosen by the force is detailed at **Appendix A**.
6. If caller line identification is operated, central stations must not bar this facility on police calls.
7. If a stamped, addressed envelope (SAE) is required with the URN application this will be listed at Appendix A.

These administration charges do not represent a charge for our attendance at alarm calls, nor do they form a contract with the occupier of the premises for response to calls.

ACPO Security Systems Policy April 2004
ACPO SECURITY SYSTEMS POLICY

APPENDIX F

**NOTICE OF:
 VARIATION REASON(S):**

	Installation Date:
	Variation Date:

INT URN	1
P/A URN	2
URN	3

NAME OF ALARM RECEIVING CENTRE
Police Ref:
Address

NAME OF INSTALLER
Police Ref:
Address

NAME OF MAINTAINER
Police Ref:
Address

DETAILS OF PROTECTED PREMISES

HOUSEHOLDER	Title: _____ Surname: _____ Business Name: _____ Trading Name (if different): _____	Initial(s): _____	
Address:			
Address:			
Town:			
County:			
Postcode:		(incl STD code)	
		E-mail address	
Type of Premises:			
If other, state:	O/S Grid Map Ref FIG _____		
Directions from main road: (Rural / new sites)			

TYPE OF SYSTEM

TYPE OF CONFIRMATION

ADDITIONAL FEATURES

TYPE OF SIGNALLING	
Primary	
Secondary	

STANDARD TO WHICH INSTALLED

EXISTING URN NO.			
Int		CCTV	
PA		Veh tracking	

PREVIOUS USER (Company name when applicable)

ADMIN FEE	SOUNDER DELAY

CONTRACT NO: _____

Signed: _____
Print Name: _____
Position in company: _____
Date: _____

If this form is not completed as appropriate or the Hazard and Site Risk statement or the fee is not enclosed it will be returned unprocessed

POLICE USE ONLY

ACPO SECURITY SYSTEMS POLICY**KEY TO COMPLETION OF APPENDIX F DOCUMENT**

Select the type of notice, from 1 to 3.

Then select the appropriate data, i.e. if number 1 is selected, you will need to choose data from the headings marked with a 1.

Note: If number 3 is selected choose data relevant to the variation.

- | | | |
|-------------------|----|---|
| NOTICE OF: | 1. | Application for a Unique Reference Number (URN). |
| | 2. | Application to reinstate a Unique Reference Number (URN). |
| | 3. | Variation to an existing security system. |

TYPE OF SYSTEM (1)
Intruder Alarm
Personal Attack
Combined IA/PA
CCTV
Vehicle tracking

TYPE OF CONFIRMATION (1 2 3)
Audio
Visual
Sequential
Audio and Sequential
Visual and Sequential

ADDITIONAL FEATURES (1 2 3)
None
Smoke Generator
CCTV
Lighting
Chemical trace
Access control

TYPE OF SIGNALLING (1 2 3)
Digital Communicator
Monitored Line
Direct Line
Radio
Dual Signalling

ADMIN FEE (1 2 3)
Applicable
Not Applicable

STANDARD TO WHICH INSTALLED (1)
BS 4737
DD:243
BS 4737 + DD: 243
BS 7042
BS 6799 Class VI
BS EN 50131
BS EN 50132
BS 8418

TYPE OF PREMISES (1)
Retail
Commercial
Public Sector
Licensed
Domestic
Industrial
Bank or Financial
Institutional
Other

VARIATION REASON(s) (1 2 3)
Upgrade to confirmation
Signalling amendment
New user
Change of user name
Address amendment
Additional features
Takeover from another maintainer
Change of Alarm Receiving Centre
Maintenance contract cancelled
System removed
Change of sounder delay

SOUNDER DELAY (1)
0 Minutes
5 Minutes
10 Minutes
15 Minutes

HAZARDS AND SITE RISK STATEMENT (HEALTH & SAFETY)

THIS FORM IS CONFIDENTIAL AND MUST BE COMPLETED AND SIGNED BY THE OCCUPIER

Police Officers will not normally enter the premises without the keyholder. However, this may on occasions be necessary due to suspicious circumstances. In order that attending Police Officers may be pre-warned, you are required to state any site hazards or risks.

The following list is not definitive but intended as a guide to some of the most common types of hazards. You should carefully consider your premises and grounds to identify any other risks or hazards and record them under "OTHERS".

MY SECURITY SYSTEMS COMPANY NAME IS:

.....

The following applies to the building(s) and grounds of these premises:

POND	✓	DOGS	✓
SWIMMING POOL		DANGEROUS ANIMALS	
RIVER FRONTAGE		FIREARMS	
GLASS COPING WALLS		AMMUNITIONS	
RAZOR WIRE		EXPLOSIVES	
INSPECTION PITS		DANGEROUS MACHINERY	
SETTLEMENT TANKS		GAS CYLINDERS	
VATS		TOXIC MATERIALS	
BASEMENT		CONTAGIOUS SAMPLES	
FRAGILE ROOF		FLAMMABLE SUBSTANCES	
DANGEROUS STRUCTURE		FUEL STORAGE	
LOW CEILING BEAMS		CHEMICALS	
SLIPPERY FLOORS		RADIO ACTIVE MATERIALS	
FURNACE		ASBESTOS	
ELECTRICITY SUB-STATION		SPRINKLER SYSTEM	

OTHERS:

IF NO SITE HAZARDS OR RISKS, STATE NONE:

Name of Occupier / Premises			
Address			
County		Postcode	

I confirm that the Alarm Receiving Centre has been given details of two keyholders capable of attending within 20 minutes of notification. I am aware that persistent failure unjustifiably of keyholders to attend within that time may result in the withdrawal of police response and/or approval for the system.

Signed:		Print Name:	
----------------	--	--------------------	--

If commercial business;

State position in Company:		Date:	
-----------------------------------	--	--------------	--

POLICE ADMINISTRATION FEE (if applicable) MUST BE ENCLOSED WITH THIS FORM AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY– CHEQUES/POSTAL ORDERS SHOULD BE MADE PAYABLE TO YOUR LOCAL FORCE POLICE AUTHORITY. **PLEASE DO NOT SEND CASH**

The administration charge does not represent a charge for our attendance to activations of your security system nor does it form a contract with the occupier of the premise for response to activations
Should site hazards and risk circumstances change you must update our records (free of charge).

Data Protection Act 1998
 Personal data supplied on this form may be held on, and/or verified by reference to information already held on computer.

POLICY COMPLIANT COMPANIES – POLICE ADVICE TO PUBLIC

The police List of Compliant Companies is for police administration purposes only.

Members of the public seeking information on security system companies shall be advised as follows:

The Police accept installations of remote signalling alarms from alarm companies whose business is subject to inspection by independent inspectorate organisations as identified by the police service nationally. Currently these are:

NSI (National Security Inspectorate), Queensgate House, 14 Cookham Road, Maidenhead, Berkshire, SL6 8AJ. Telephone 0870 2050000

SSAIB (Security Systems & Alarm Inspection Board), Suite 3, 131 Bedford Street, North Shields, Tyne & Wear, NE29 6LA. Telephone 0191 296 3242.

These organisations publish lists of approved companies. I suggest that you seek answers to the following questions before deciding upon a particular company:

- a) Before disclosing personal security details, have I checked the address and credentials of the company and seen proof of identity from their representative.
- b) Is the company subject of an independent inspection process and if so, which organisation.
- c) Is the installation of an alarm a requirement of my insurance company and if so, is the company acceptable to my insurer.
- d) Can the company representative provide me with a list of police rules for occupiers of premises with alarm and written confirmation that the alarm and the company are currently acceptable to the local police for the transmission of alarm messages from new installations.
- e) Have I sought written quotations from at least two alarm installers.
- f) Does the quotation:
 - (i) specify that the installation will be to BS EN 50131-1, BS4737 or BS 7042 (high security systems) or, if it is a wire free alarm, BS 6799, or BS8418 for a detector activated CCTV system.
 - (ii) Include the terms of maintenance and monitoring contracts.
- g) Does the company operate a 24 hour call-out service and emergency attendance within 4 hours.

APPENDIX I

Letter to be handed to potential customers by all companies installing security systems.

Dear Sir/Madam

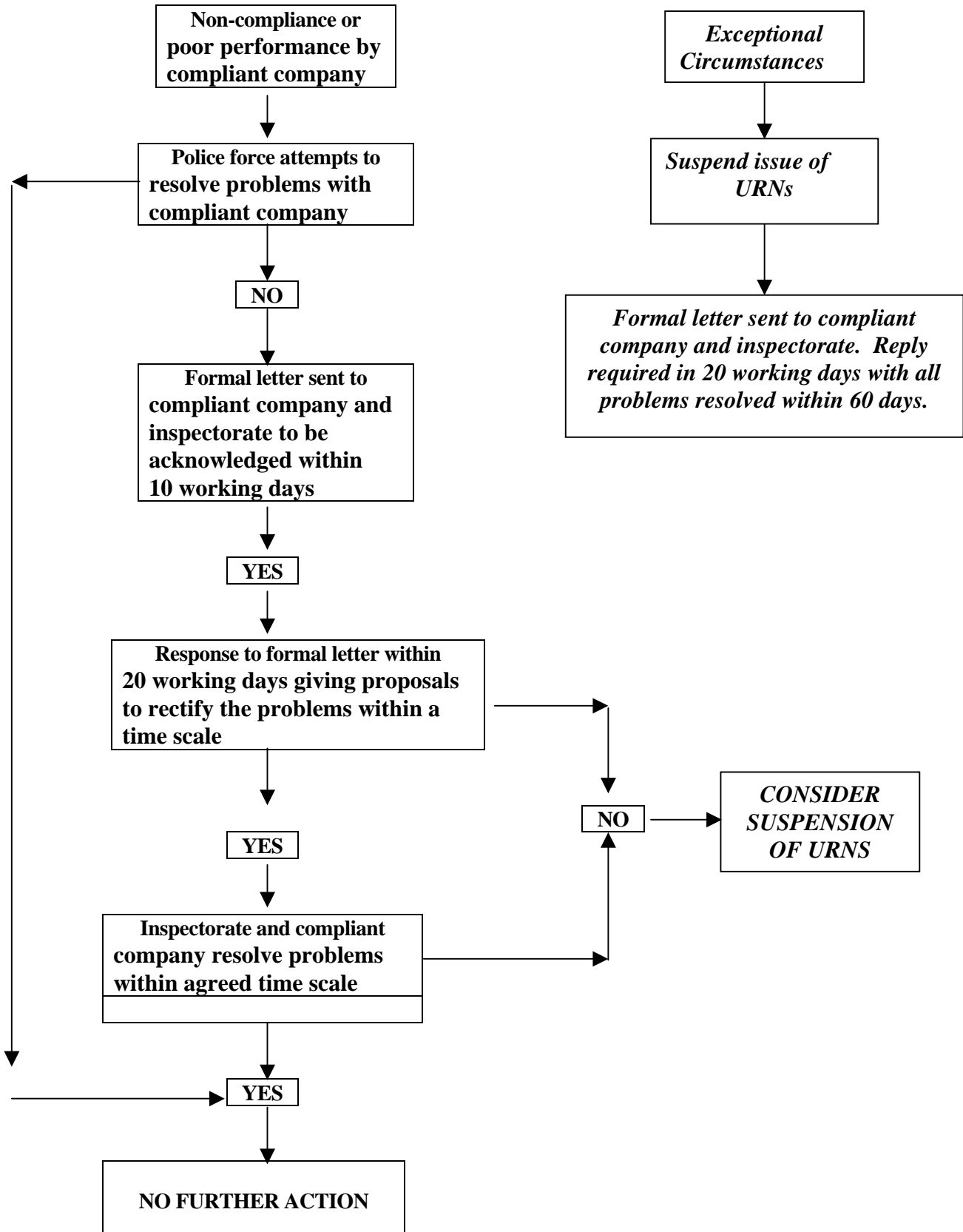
A properly installed security system will help to protect your premises when it is unoccupied. As you are considering the installation of a remote signalling security system you should be aware that the police have safeguards to reduce levels of false calls which divert us away from other tasks in your community.

To avoid misunderstanding, here is a précis of the conditions. However, should you require further information please contact your local Crime Prevention Officer.

1. Installation, maintenance and monitoring of security systems must only be undertaken by companies acceptable to your local police.
2. Such acceptance by the police does not imply guarantee of the company's work. You should seek confirmation from the company that it is compliant with police policy and is acceptable to the Police Force for the transmission of alarm messages from new installations.
3. You will receive training on the operation of the system by the installer including methods of cancelling accidental operations of the alarm.
4. Commercial premises may be required to have a 10 minute delay of sounders to give us the opportunity to attend and detain offenders. You may apply to Police Headquarters for exemption to the delay.
5. Any external audible sounder should cut out after 20 minutes and alarms causing annoyance under the terms of the Control of Pollution Act may result in prosecution. Some Local Authority areas may be subject of Section 9 of the Noise & Statutory Nuisance Act 1993, or in London The London Local Authorities Act 1991 (Misc Provisions) which places additional responsibilities on the occupier. Please check with the installing company, or your local Council for details.
6. Security systems will receive a police response determined by the nature of demand, priorities and resources which exist at the time. After 2 false calls in any 12 months you will be advised in writing so that you may take remedial action, but subsequent calls may receive a lower priority.
7. Following 5 false calls in any rolling 12 months, police attendance will be withdrawn. We will continue to attend personal attack alarms where these are identified separately by the alarm receiving centre provided the attack alarm does not generate a total of 5 false calls.
8. Police attendance may be restored if written application is made following 3 months free of false calls or when the system has been upgraded to current policy requirements. The application must be supported by written evidence from your security company. It is therefore in your interest to identify and correct the cause of any false alarm at the earliest opportunity.
9. On completion of the administration procedures your security company will be issued with a Unique Reference Number (URN) which identifies your system within our files to speed call handling. This number should be used in all correspondence to the police but please do not disclose it to any unauthorised person.
10. There is a requirement to have at least two keyholders, details of whom will be maintained by the Alarm Receiving Centre. Keyholders shall be trained to operate the security system, be telephone subscribers, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified.
11. In accordance with the Data Protection Act 1984 personal information relating to you and your keyholders in connection with the security system may be held on a computer. Please ensure that relevant names and addresses are current.

It is regretted that such constraints are imposed but they are essential if we are to maintain the credibility of alarm systems, reduce false calls and provide you with an acceptable service.

MEMORANDUM OF UNDERSTANDING



POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION**APPENDIX K**

Dear Sir/Madam,

We are pleased to note that you are having a security system installed at your premises. Every possible attention is paid to calls emanating from such systems but in this connection we must seek your co-operation on the following important matters. Failure to comply with any of the following conditions may result in the police withdrawing response from your system.

You are advised that police personnel may have withdrawn from the premises before the arrival of a keyholder. In this case the keyholder may contact the police and ask them to attend if there is evidence of an offence.

1. FALSE ALARMS

Because of the considerable amount of time expended attending false calls, the Police have formulated the following policy:

Every user having a system which produces two false calls within a period of 12 months, shall be served with a notice requiring action to be taken to prevent further false calls. If, when subsequent calls are received, we have other high priority calls to contend with, police response may be delayed whilst we deal with those calls.

Should more than four such calls be received within any 12 month period, police response shall be withdrawn for a minimum period of 3 months free from false calls.

Will you therefore please ensure that those involved in the operation of your security system are familiar with its functions and are informed of the importance of avoiding its accidental operation. Also, in the event of technical faults, please inform your system maintenance company as soon as possible after the fault has become apparent.

2. ENGINEER RESET

The current standard to which your security system company must comply, states that following activations, resetting of the system shall be undertaken by means not normally available to the customer i.e. engineer reset or by alarm receiving centre.

3. NOISE NUISANCE

Your attention is also drawn to the Code of Practice on Noise from Audible Intruder Alarms 1982, issued under the Control or Pollution Act 1974, in respect of noise, nuisance and keyholder response. This includes a 20 minute limit on the operation of audible warning devices.

4. PERSONAL ATTACK ALARMS

The new Security Systems Policy states "A personal attack may be operated to summon urgent police assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that defined area". However in many instances PAs are used where there is no threat to persons within a defined area. Without knowing the circumstances under which the PAs are activated, the police must respond. You should be aware that in the current policy, if you use the PA five times in a rolling twelve month period and there is no threat to persons in a defined area, you will lose police response for a period of time.

Accidental misuse happens when staff are not trained in the use of a PA or visitors to the premises have access to the PA and press it out of curiosity. It is important that the PA is placed where members of the public cannot have access. Accidental misuse also occurs where duress codes are used. This is when a member of staff enters the duress code instead of the normal set or unset code. To prevent this happening all staff (including cleaning staff) who have access to the codes should be properly trained in the use of duress codes.

Accidental misuse of your PA system could cause you to lose police response. Guard against this possibility.

The following are examples of intentional but non-essential operation of a PA activation:

- a) Garage forecourt attendant when someone has driven off without paying for petrol.
- b) Shopkeeper because someone leaves the store without paying for goods.
- c) Householder or publican who sees a fight in progress.
- d) Householder who hears a suspicious noise outside

A PA is there to summon police assistance when you are threatened. DO NOT use it for any other purpose

5. DATA PROTECTION ACT 1984

Personal data supplied may be held on and/or verified by reference to information already held on computer.

Should you require further advice, please do not hesitate to contact this office.

Yours faithfully,

NOTICE OF URN TO INSTALLER

Dear Sir/Madam,

RE: _____

I acknowledge receipt of your recent Notice of Intention to Install a Security System at the above address.

Details of activations received at your Alarm Receiving Centre/Remote Video Response Centre should be passed to the _____ Police Force Call Handling Centre on _____. The message must include the Unique Reference Number _____ for use in the Call Handling Centre and failure to quote the URN will result in Police attendance being refused.

THE UNIQUE REFERENCE NUMBER MUST BE QUOTED IN ALL FUTURE CORRESPONDENCE RELATING TO THIS INSTALLATION.

It is a requirement of the _____ Police that all security systems installed should meet the British Standard BS EN 50131-1, BS 4737, BS 7042, BS 6799 or BS 8418 and Codes of Practice identified in the Policy and that the installing company issue a certificate to that effect.

Re-setting of intruder alarm systems should be carried out only by a representative of your security systems company. Please note instant bells are permitted on residential premises/a ten minute bell delay will be required at this location/instant bells will be permitted at this location.

Yours faithfully,

LETTER TO BE FORWARDED TO SUBSCRIBER AT TWO FALSE CALLS

Dear Sir/Madam,

Security systems are only one example of the demand placed on the Police Service for an immediate response. False calls significantly outnumber genuine calls and divert police resources.

In an effort to reduce the unacceptably high number of false calls received by the Police, it has been necessary to introduce a policy governing the installation, maintenance, monitoring and use of security systems. The policy includes a close monitoring of all calls. Records indicate that there appears to have been at least two false calls from the system at your premises within a twelve-month period. In view of this, you are advised to contact your security systems company at the earliest opportunity in an effort to resolve what appears to be a problem with your security system or its operation.

The current level of false calls means that priority may be given to other urgent calls for our assistance and response to your alarm may therefore be delayed. For your security system to return to the original high priority response, it must be free of false calls for three months or the system upgraded to comply with current policy requirements. Should you require further information concerning this upgrade, please contact your security systems company.

Regrettably, should the false calls persist, it will be necessary to consider the withdrawal of Police response to activations from your system, a situation we would wish to avoid with your co-operation.

You are advised to contact your Insurance Company and inform them of the contents of this letter as soon as possible as your insurance cover may be affected.

This information is brought to you with the assistance of your security company. Should you have any queries in respect of this letter, please contact your alarm company in the first instance, quoting your Unique Reference Number.

Yours faithfully,

Copy to: Security System Company

LETTER FROM POLICE TO CUSTOMER ADVISING WITHDRAWAL OF RESPONSE

Dear Sir/Madam,

I refer to previous correspondence concerning the operation of the security system at your premises.

Regretfully, continued monitoring of your security system has indicated that further false calls have been received.

Following careful consideration I have to inform you that Police response will no longer be given to your security system after the _____ . Reinstatement of response can be considered following notification from your security company that a system with confirmed technology has been installed and that only confirmed activations will be passed to the police. The system must also comply with BS DD243 (2002). If you already have a confirmed system, your security company may apply for reinstatement of response when they are able to provide evidence that a three month period free from false calls has been achieved. Should you have any queries concerning confirmed technology, please speak to your security company.

During the period of withdrawn response, your keyholder will continue to be informed of all activations by your monitoring station.

As the Police response is about to be withdrawn, I must point out that this action could affect any insurance cover you may have relating to the premises. You are therefore advised to contact your Insurance Company and Security System Installer and advise them of the contents of this letter as soon as possible.

Yours faithfully,

Copy to: Security System Company

REINSTATEMENT OF POLICE RESPONSE LETTER

Dear Sir/Madam,

RE: _____

Further to your correspondence dated _____, the situation has now been reviewed.

I am able to inform you that police response to calls received from your security system at the above address has been reinstated to level 1 with immediate effect.

This decision however, must be made without prejudice on our part to again reducing response should a high incidence of false calls occur or should you fail to comply with the police Security Systems Policy.

I trust that the action you have taken will continue to be effective and may I thank you for your efforts in this matter.

Yours faithfully,

WITHDRAWAL OF UNIQUE REFERENCE NUMBER – LETTER TO SUBSCRIBER

Dear Sir/Madam,

I refer to previous correspondence regarding the withdrawal of Police response from the above security system.

Response has remained withdrawn for a period in excess of 6 months and it has not been possible to reinstate response. Consequently a decision has been made to withdraw from monitoring the system with effect from the _____.

Your security system company has been instructed not to pass any further calls to the police after that date.

Advice regarding alternative means of security may be available from your local Crime Prevention Officer.

Yours faithfully,

WITHDRAWAL OF UNIQUE REFERENCE NUMBER – LETTER TO SECURITY SYSTEM COMPANY

Dear Sir,

RE: _____

As a direct result of poor system performance, police response was withdrawn from the above system on the _____, and has remained withdrawn for a period in excess of six months.

Consequently, a decision has been made to withdraw the Unique Reference Number with effect from the _____.

After that time, further calls must not be passed to the Police. Your client is fully aware of the situation.

Yours faithfully,

REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS

1. INTRODUCTION

- 1.1 This document sets out the police requirements for remotely monitored detector activated CCTV systems to enable such systems to gain Unique Reference Numbers (URN) from police forces.
- 1.2 Companies monitoring remotely monitored detector activated CCTV systems, known as Remote Video Response Centres (RVRC) and Installers will ensure that these police requirements are brought to the attention of the users of such systems that require a police response.
- 1.3 Remotely monitored detector activated CCTV systems that are installed and monitored to the requirements stated in this policy, will be known as Type A systems and will be issued with a Unique Reference Number (URN).
- 1.4 Systems for which police attendance may be required and which operate outside the procedures identified in the policy, will be known as Type B systems. Unique Reference Numbers (URN) will not be issued to these systems.
- 1.5 The levels of police response to suspected crime reported by a Type A remotely monitored detector activated CCTV system, will be the same as that stated in the ACPO Security Systems Policy clause 3.1.

2. STANDARDS

- 2.1 Installers of remotely monitored detector activated CCTV systems will comply with all of the following standards and guidelines:
- ACPO Security Systems Policy
 - BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice
 - BS EN 50132-7: CCTV Application guidelines
- 2.2 RVRCs monitoring detector activated CCTV systems will conform to all of the following standards:
- BS 5979 (Cat II):
 - BS 8418: Installation and remote monitoring of detector activated CCTV systems – Code of Practice

3. LEGAL REQUIREMENTS

- 3.1 Any remotely monitored detector activated CCTV system that requires police response will be installed and monitored in such a way as to ensure that any criminal activity recorded can be supported by correct operational procedures. It is recommended that all organisations draw up procedures to ensure compliance with the Data Protection Act 1998 and, where applicable, the Human Rights Act 1998.

4. PROCEDURES

- 4.1 The relevant police force will be sent a notice to install a remotely monitored detector activated CCTV system using Appendix F of the ACPO Security Systems Policy. A URN will be issued in line with the relevant police force policy (Appendix A of the ACPO Security Systems Policy refers).
- 4.2 The means of image collection and communication between the premises and the RVRC is a matter for the installer and the RVRC. However, the system will be installed to meet the requirements of Clause 2 of this appendix.
- 4.3 The system will be maintained in accordance with the BS 8418 Clause 13.1, and the requirements of the Data Protection Act 1998, CCTV Code of Practice (latest edition).

APPENDIX R (continued)

- 4.4 The system will have the capability of audio challenge, which is to be used if appropriate. Local environmental conditions will be taken into consideration.
- 4.5 The RVRC will only call the police if there is sufficient evidence in the images of unauthorised access to the site/premises and of actual criminal activity in progress.
- 4.6 The RVRC operator will provide sufficient location and criminal activity information to the police control room.
- 4.7 The RVRC will employ filtering techniques to avoid unnecessary calls being passed to the police.
- 4.8 Any images required by a police force for investigative purposes will be supplied upon request.
- 4.9 The RVRC will send the recorded evidence (or at least a working copy) in the first instance to the investigating officer, with a completed statement of evidence to show continuity.
- 4.10 RVRCs using digital recording methods will adhere to the procedures for processing digital images, issued jointly by the Home Office, ACPO and PSDB.

5. MANAGEMENT INFORMATION

- 5.1 RVRCs will provide management information that is compatible to ACPO in relationship with the systems for analysis.
- 5.2 The information supplied will give a detailed analysis of the total number of calls passed to the police, registered with the URN.
- 5.3 Remotely monitored detector activated CCTV systems will be subject to the same conditions as laid down in the ACPO Security Systems Policy (Clause 3 refers) for the relevant police forces in relation to the total number of incidents incorrectly passed to the police.
- 5.4 The Memorandum of Understanding (MOU) is applicable to CCTV systems.

6. INDEMNITY

- 6.1 This document does not impose any liability on any police force, its officers or the police authority arising out of the failure or timeliness in responding to an activation from a remotely monitored detector activated CCTV system.

July 2003

REQUIREMENTS FOR SECURITY SYSTEM SERVICES

Association of Chief Police Officers (England, Wales and Northern Ireland) and The Association of British Insurers

Requirements for Security System Services

- I For the issue of a unique reference number (urn) by police forces in (England Wales and Northern Ireland), and/or to meet the minimum general recommendations for member companies of the Association of British Insurers, the installation / services provided by the Installation, Maintenance or Monitoring Company shall be certified in accordance with the provisions of this document by a certification body accredited to EN 45011 by United Kingdom Accreditation Service.
- II The Certification Body shall -
- a. Be a company limited by guarantee and not having a share capital. The company is to be formed in accordance with the relevant Companies Act identified in Annexe A.
 - b. Ensure the company law members/guarantors of the certification body shall be limited companies properly formed in accordance with the relevant Companies Acts identified in Annexe A or suitable individuals.
 - c. Ensure the memorandum and articles of association and their company law members/guarantors are specific to a certification body and identify the objects of a properly constituted certification body.
 - d. Provide audited accounts, where applicable, or such other accounts as are mandatory under Company Law, to show compliance with Clause 4.2(i) BS EN 45011: 1998
 - e. Carry out surveillance of certified service providers in accordance with the provisions of paragraph III. Surveillance shall be conducted at a minimum frequency of once per year and for installation companies, this surveillance shall include an inspection/functional test of installation(s) for compliance with the appropriate documents identified in Annexe A
 - f. Have documented procedures for the inspection and test of installed and maintained systems to ensure compliance with the appropriate documents identified in Appendix A.
 - g. Ensure personnel who have access to third party security arrangements as a result of this process shall be subject to a security vetting procedure to British Standard 7858 or an equivalent, which identifies any unspent convictions or associations which may be deemed unacceptable.
 - h. Be required to establish if certification has been given and/or withdrawn by any other Certification Body accredited to this scheme when an Installation, Maintenance or Monitoring Company makes application for acceptance.
 - i. Where disciplinary action is pending, in process or has resulted in expulsion by Certification Body 'A' of an Installation, Maintenance or Monitoring Company, for non-compliance with documents identified in Appendix A, the non-compliance causing the disciplinary action must be resolved prior to approval by another Certification Body 'B'.
 - j. Deal with any complaint against an Installation, Maintenance or Monitoring Company made by a police force in England, Wales & Northern Ireland or member company of the Association of British Insurers, in accordance with the Memorandum of Understanding identified in Annexe A.
 - k. Invite a member of the Association of Chief Police Officers (England, Wales & Northern Ireland) Intruder Alarms Group and the Association of British Insurers, to attend board meetings as an observer for agenda items relating to this scheme.

APPENDIX S (continued)

- I. Be invited to the Association of Chief Police Officers (England, Wales & Northern Ireland) – Security System, Industry Liaison, Group Meetings and/or relevant meeting held by the Association of British Insurers as and when deemed necessary by the Association.

III Installing, Maintaining and/or Monitoring Companies

The installing maintaining and/or monitoring company, commensurate with the services they provide, shall -

- a. Vet personnel who have access to third party security arrangements in accordance with British Standard 7858, which ensures personnel of good repute and identifies any unspent convictions or associations, which may be deemed unacceptable.
- b. Have financial stability to trade, at present and in the future.
Guidance - The certification body in determining financial stability to trade, may consider checking bank references, court orders and annual accounts prepared by an independent accountant, i.e. as provided to the inland revenue. In the case of an incorporated company the audited annual accounts or such accounts as are statutorily required should a company be exempt from audit.
- c. Have adequate and relevant insurance in respect of employers, product, public, efficacy and wrongful advice liability.
Guidance - Insurance cover to a minimum of £1,000,000 per incident.
- d. Have competent management with responsibility for all services provided.
Guidance – Management must be conversant with the relevant standards for the services they provide and be competent to inspect and test systems. Their responsibility extends to services provided by sub-contractors who must comply with all aspects of this document.
- e. Have sufficient competent staff to carry out their contractual demands and the requirements of standards.
Guidance – The contractual demands and requirements of standards includes the design, planning, installation, system performance, operation, commissioning, false alarm management, complaint handling, maintenance and repair for intruder alarms in accordance with the appropriate documents in Annexe A.
- f. Have adequate arrangements, documented procedures and systems in place for all of their activities.
Guidance – This covers all aspects of a companies installing, maintaining and monitoring activities and includes –
 - *Personnel (includes vetting, competence, qualification)*
 - *Sales (includes enquiry, survey, quotation, order)*
 - *Installation (includes design planning, commissioning, training of subscribers)*
 - *Maintenance (includes preventative and corrective)*
 - *System performance*
 - *Confidentiality*
 - *Handling of system activations, e.g. intruder alarm filtering*
 - *Complaint handling**The documented procedures are to the extent necessary to achieve consistency of application, in the case of NSI companies they will require a certificated quality management system. Complaint handling needs to show logging, corrective action and review procedures.*
- g. Have suitable premises where confidentiality can be observed and with adequate safeguards for security of information on a 24 hour basis.
Guidance – Any means of electronic security protection used for this purpose shall comply with the minimum standards of these procedures. Alarm receiving centres and/or monitoring centres must comply with the appropriate standards in Annexe A.
- h. Have the necessary resources to support those activities.
Guidance – The necessary resources extends to all that are necessary to provide the services offered e.g. tools, test equipment, vehicles, office equipment, spares, personnel etc.
- i. Have sufficient systems installed and/or monitored to enable competence and trading history to be determined.

APPENDIX S (continued)

- j. Have immediate access to and comply with the standards and documents identified in Annexe A.
- k. Have customer contracts describing the products and services to be supplied together with the associated terms and conditions.
*They are to be fair and reasonable, describe the products and services to be provided, show title to any equipment, describe the terms of the warranty and detail **all** the charges applicable.*
- l. Not engage in pressurised selling or unfair business ethics.

IV New standards and documents applicable to this scheme will be notified by the Secretary to the Association of Chief Police Officers (England, Wales & Northern Ireland) Intruder Alarm Group or the Association of British Insurers to all Certification Bodies accredited to this scheme.

V Where amendments to this scheme are deemed appropriate by the Association of Chief Police Officers and/or the Association of British Insurers a consultation meeting will be instigated for attendance by those concerned.

ANNEXE A**British Standards and European Norms (Latest Issue)**

BS 4737	Intruder Alarms in Buildings
BS 7042	High Security
BS 8418	CCTV Systems
BS 5979 (Cat II)	Alarm Receiving Centres
BS 6799	Wire free Alarms
BS 7858	Vetting of Security Personnel
PD 6662	Scheme for the implementation of European Standards
BS EN 50131-1	Alarm systems – Intrusion Systems – General requirements
BS EN 50131-6	Alarm Systems – Intrusion Systems – Power supplies
BS EN 50136-1-1	Alarm transmission systems – General Requirements
BS EN 50136-1-2	Alarm transmission systems – Requirements for systems using dedicated alarm paths
BS EN 50136-1-3	Alarm transmission systems – Requirements for systems with digital communicators using the public services telephone network
BS EN 50136-1-4	Alarm transmission systems – Requirements for systems with voice communications using the public services telephone network
BS EN 50132-7	Alarm systems – CCTV surveillance systems used in security applications – Application guidelines
BS 7939	Smoke Security Devices

British Standard Institute Drafts for Development (Latest Issue)

BS DD 242	High Security
BS DD 243	Automatic Re-Arming, Filtering and Substantiating Alarm Information
BS DD 244	Wire Free Alarms
BS DD 245	Management of False Alarms
DD CLC/TS 50131-7	Alarm Systems – Intrusion Systems – Application Guidelines

Legislation

Noise and Statutory Nuisance Act 1993, Section 9 and Schedule 3 sets out requirements for intruder alarms, keyholders and noise. (As adopted)

Control of Pollution Act 1974, sets out requirements for noise and 20 minute limit for audible warning devices.

The Companies Act 1985 and 1989

Association of Chief Police Officers (England, Wales & Northern Ireland)
Security Systems Policy 2004

Memorandum of Understanding. (Dated: December 2001)