# Police Requirements & Response to Security Systems

The National Police Chiefs' Council (NPCC) has agreed to these revised guidelines being circulated to, and adopted by, Police Forces in England, Wales & Northern Ireland.

It is NOT PROTECTIVELY MARKED under the Government Protective Marking Scheme and any referrals for advice and rationale in relation to Freedom of Information Act disclosure should be made to the NPCC Central Referral Unit at npcc.request@foi.pnn.police.uk.

# Document information

| | |
|---|---|
| **Protective marking:** | NOT PROTECTIVELY MARKED |
| **Author:** | CC Steve Watson |
| **Force/Organisation:** | South Yorkshire Police |
| **NPCC Coordination Committee Area:** | Crime Operations |
| **APP/Reference Material** | Reference Material |
| **Contact details:** | 0191 375 2265 |
| **Review date:** | April 2019 |

These revised requirements have been produced and approved by the NPCC Crime Operations Coordination Committee. Requirement produced by the NPCC should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The operational implementation will require operational choices to be made at local level in order to achieve the appropriate police response and this document should be used in conjunction with Authorised Professional Practice (APP) produced by the College of Policing. It will be updated and re-published as necessary.

Any queries relating to this document should be directed to either the author detailed above or the NPCC Business Support Office on 020 7084 8959/8958.

Summary of Amendments to previous document **Guidelines on Police Requirements & Response to Security Systems** 2015 version (not part of the requirements):

The document has been retitled the **National Police Chiefs' Council (NPCC) Police Requirements & Response to Security Systems**

| | |
|---|---|
| 1.2 | Amendment to paragraph. |
| 1.3 | Amendment to paragraph. |
| 2. | Guidance, Advice and procedures changed to Requirements and Procedures. |
| 2.1.1 | Additional of BS 8591. |
| 2.1.2 | Amendment to paragraph. |
| 2.2.1 | New Requirement. |
| 2.3.2(e) | Chief Officer of Police replaced with "relevant police force". |
| 2.5 | Amendment to clarify requirements for Type A Security Systems. |
| 2.6.1 | All submissions to be sent to the relevant police force, not the chief officer of police. Additional sentence to obtain/locate correct police force for submission of appendix F. |
| 2.6.2 | Addition to sentence to reference Appendix A – Force Service Standard. |
| 2.7.1 | Addition to sentence to reference Appendix G. |
| 2.8.1 | Additional sentence covering Keysafe devices. |
| 2.8.3 | Addition of the British Standard in relation to keyholding and response. |
| 2.10.1 | Addition of the British Standard in relation to false activation management. |
| 2.10.2 | d) & e) removed. |
| 2.10.3 | Additional requirement. |
| 2.10.4 | Additional requirement. |
| 2.10.5 | Additional requirement. |
| 2.10.6 | Additional requirement. |
| 2.11.1 | Additional wording not to misrepresent the cost of a URN to clients. |
| 2.11.6 | Additional requirement. |
| 2.12.1 | Addition to sentence with reference to activations caused by engineers. |
| 3.2.3 | Additional sentence at end of paragraph. |
| 3.2.4 | (i) Change of wording. |
| 3.4.2 | Amendment re specification requirement form – Addition of Annexe B of Appendix F. |
| 3.4.4 | Additional sentence re notification of withdrawal to the ARC. |
| 3.4.5 | Addition to requirement – Call back confirmation is no longer an acceptable form of confirmation for commercial premises. |
| 3.4.6 | Amendment to sentence. |
| 3.5.2 | Removal of last sentence. |
| 3.6.1 | Amendment to sentence. |
| 3.6.3 | Addition to paragraph to cover 3rd part monitoring. |
| 3.6.5 | Amendment to sentence – may not is replaced with unlikely. |
| 3.6.6 | Additional Requirement. |

| | |
|---|---|
| 4.1 | DPA 2018 & GDPR Requirement added. |
| 4.3.1 | Re-worded. |
| 4.5.1 | Additional sentence. |
| 4.5.2 | Amendment to paragraph. |
| 4.5.3 | Amendment to paragraph. |

| | |
|---|---|
| Appendix B | Changed from Policy Requirements to Police Requirements Document and change of layout. |
| Appendix C | Addition of “monitoring centres” to opening paragraph. |
| (iv) | Removal of criteria after the word employment. |
| (v) | Application submission to the alarms administration office not the Chief Constable. |
| Form A | Removal of gender data and maiden name request. Title request added. |
| Form B | .Replace policy with requirements. |

Appendix E

| | |
|---|---|
| 2. | Addition – the customer will be informed of URN cancellation due to non-payment of the administration fee. |

Existing System Takeover

| | |
|---|---|
| a) | Addition of legal entity. |
| c) | Addition of security company taking over an existing system. |

| | |
|---|---|
| 4. c) | Addition of legal entity. |
| 5. | Chief constables replaced with the respective force. |
| 8. | Removed. |
| 9. | Removed. |

| | |
|---|---|
| Appendix F | removal of signature (electronic signature will suffice). |
| Annexe A 3) | Replacement of ban with withdrawal. |

Annexe B

| | |
|---|---|
| a) | Clarification – call back confirmation available to domestic/residential premises only. |
| Note 2. | Multi action hold up devices are not allowed for the restoration of police response when the initial method of confirmation has failed. |
| Note 2 | Paragraphs a) and b) removed. |

| | |
|---|---|
| Note 1. | First line, the word replace inserted after implemented. Second paragraph removed. |
| Annexe C | Standards Matrix updated. |
| Appendix G | Replaced – new user friendly document created. |

| | |
|---|---|
| Appendix H | The word automatic removed from fifth paragraph. (g) addition; only pay for one year’s monitoring in advance. Last Paragraph reference to consumer direct removed and replaced by www.gov.uk/consumer-protection-rights and details for Citizens Advice. |

| | |
|---|---|
| Appendix I | |
| Clause 5 | Re-written to include Clean Neighbourhood and Environmental Act 2005. |
| Appendix K | |
| 4. | Removal of paragraph in relation to duress codes causing false activations. |
| Appendix L | Removal of dated standards requirements. Removal of sounder bell requirements. |
| Appendix M | Document title amended from subscriber to customer. |
| Appendix P | Document title amended from subscriber to customer and re-wording of letter. |
| Appendix Q | Re-wording of letter. |
| Appendix R | . |
| 2.1 | Bullet point 3 – additional standard added BS EN 67676-4 |
| 2.2 | Additional standard added - BS8951:2014 (Cat II) or BS EN 50518 |
| 4.3 | Add ICO to CCTV Codes of Practice. |
| 4.5 | Sentence re-worded. |
| 5.1 | Sentence re-worded. |
| 5.4 | Paragraph removed. |
| Appendix S | |
| I | Amend EN 17605:2012 to BS EN 17065:2012. |
| III b. | Addition to trade lawfully; ethically and comply with the Consumer Contracts Regulations Act 2013. |
| III c | New guidance on insurance cover. |
| III l. | Replace paragraph with; 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. |
| III n. | Addition; Monitoring and maintenance contracts shall not exceed a period of three years and payments in advance shall not exceed one year. |
| III m | Additional sentence re compliance with the “Consumer Protection from Unfair Trading regulations 2008”. |
| Annexe A | Standards updated. |
| Appendix T | Reviewed and updated to current standards. |
| Appendix U | |
| 2.1 | Amend standard EN 17605 to EN 17065. |
| 2.4 a. | Addition of standard; BS 8591 Cat II. |
| 2.4 e. | Removal of ISO 9001 requirement. |
| 3 | Addition of DPA 2018 & GDPR. |
| 7.2 | Application submission to the alarms administration office not the chief constable. |

Appendix V

| | |
|---|---|
| 3.1 | Remove 3.1.5 and replace with 3.2 & 3.4. . |
| 3.2 | Removal of paragraph. |
| 4.2 | Addition of standard BS 8593. |
| 5.1 b | Addition of standard; BS 8591 Cat II. |
| 6 | Addition of DPA 2018. |

# Contents

## 1. PREFACE

1.1 The National Police Chiefs' Council (NPCC) recognise the rapid development of technology and its use within security systems. These requirements detail police response which is to be expected to an electronic security system as identified in the NPCC "Requirements for Security System Services".

1.2 To enable a security system to be compliant with the Requirements for Security Systems it must comply with 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, maintenance and monitoring provided by companies shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the Requirements and Response to Security Systems.

1.4 Additional operational restrictions by individual forces are listed within **Appendix A** of this document.

## 2. REQUIREMENTS AND PROCEDURES

### 2.1 Type A - Remote Signalling Systems.

2.1.1 Systems should be monitored by Alarm Receiving Centres (ARCs), Remote Video Response Centres (RVRC) and System Operating Centres (SOC). All centres must comply with BS 5979 (Cat II), or BS EN 50518 and BS8591 (Cat II).

2.1.2 Unique reference numbers (URNs) will be issued by police forces to systems monitored by these recognised centres. In the case of stolen vehicle tracking systems the URN will be allocated by NPCC Security Systems Group and issued, upon application, by police forces to the SOC not to each vehicle.

2.1.3 ARCs dealing solely with alarm systems within their 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; and
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; and
c) The security systems are operated in accordance with all other aspects of these requirements.

### 2.2 TYPE B -SECURITY SYSTEMS

2.2.1 Installation and monitoring companies that are not registered with their home force will be regarded as NON COMPLIANT. URNs will not be issued to security systems which operate outside procedures identified at Section 2.1.

### 2.3. LIST OF COMPLIANT COMPANIES INSTALLING TYPE A SECURITY SYSTEMS

2.3.1 To identify companies conforming to these requirements it is necessary for each police force to hold a list of compliant companies. Inclusion on the list does not amount to

confirmation that the company or its work has been inspected by the police. Only companies listed may install, maintain and/or monitor Type A Systems in the relevant police area. Where a company loses police recognition under these requirements, its existing customers will have 90 days in which to make alternative maintenance/monitoring arrangements.

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

(a) Be inspected and recognised by an independent inspectorate body as detailed in paragraph 1.3.

(b) Not have as a principal or employ in the surveying, sale, installation, maintenance or administration 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 in **Appendix A.**

(c) Must be on the compliant list of the home force where their main office/HQ is situated, *before* applying for inclusion on the list of other forces outside their main police force area.

(d) Once accepted will take responsibility for ensuring the company updates itself with amendments to this document, which is reviewed annually.

(e) It is a requirement that all variations to company details, including change of inspectorate shall be notified within 28 days to the relevant police force.

## 2.4 INFORMATION TO CUSTOMERS

2.4.1 The compliant list is for police administrative purposes. Members of the public seeking advice from the police about companies capable of installing remote signalling systems will be advised to seek information from UKAS accredited inspectorate bodies directly as identified in **Appendix H**.

## 2.5 NOTICE TO CUSTOMERS - TYPE A SYSTEMS

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

## 2.6 NOTICE TO INSTALL - TYPE A SECURITY SYSTEM

2.6.1 Notice of intention to install a Type A Security System requiring a URN, shall be sent to the relevant police force using the current version of **Appendices F** and **G.** (Only typed applications will be accepted). To find correct police force for application purposes go to www.police.uk Find my Neighbourhood and enter post code of premises

2.6.2 All notices or other documents required for the issue or processing of a URN may be sent by electronic means or by post. (See Appendix A – Force Service Standard).

2.6.3 This will result in the issue of a URN which must be quoted in all communication regarding the installation; the URN is issued and owned by the police. An activation received from a compliant ARC/RVRC, without a current police URN, will be treated as a

Type B system and will not receive a police response without additional evidence of an offence in progress.

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

## 2.7 VARIATIONS FROM ORIGINAL APPLICATION DETAILS

2.7.1 The relevant police force shall be notified within 28 days of **all** variations to the original URN application details and any change in maintainer and monitoring centre, in the form of **Appendix F** and **G**.
Failure to comply could lead to the Memorandum of Understanding (MOU) being implemented.

## 2.8 KEYHOLDERS

2.8.1 All premises with Type A Systems shall have at least two keyholders, details of whom will be maintained by the monitoring centre or through arrangements with a central keyholding service. The provision of a Keysafe type device is not an acceptable alternative. Keyholders shall be trained to operate the alarm, be contactable by telephone, 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 monitoring centre, not the police. Failure to comply with the above instructions could result in the URN being suspended.

2.8.2 If a keyholder is not available for any reason (e.g. sickness, holiday) a replacement must be provided to cover for any keyholder unavailability.

2.8.3 Customers who employ a commercial keyholding company must be aware of the Security Industry Authority Licensing Regulations and BS7984-1 in relation to keyholding and response.

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

2.8.5. Requests for police response should only come from the ARC's, keyholders should not contact the police asking for their attendance unless they have arrived at the protected premises and there is a crime in progress or a crime has been committed.

## 2.9 DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

2.9.1 There is no requirement for security systems to have audible or visual warning devices delayed following activation of the system. However, commercial premises may be required to have their 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**)

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

## 2.10 FALSE ALARM MONITORING

2.10.1 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. This should be done in accordance with BS8473. Companies' false alarm ratios may be monitored and forces reserve the right to suspend companies who consistently exceed the force average.

2.10.2 **Definition** – For the purpose of these requirements, a false alarm is an alarm call from a compliant system 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 HUA/lone worker/ CCTV system made with good intent.

2.10.3 Requests made by RVRC's for police to attend sightings of individual(s) seen on protected premises where no criminal activity, attempt/intent is in progress, will be considered as civil trespass and such calls would be classified as false.

2.10.4 Activation of detectors without apparent damage or entry to the premises and line faults will be considered as a false alarm unless proved otherwise.

2.10.5 When a monitoring centre attempts to cancel police attendance before a unit is deployed, the activation may be disregarded as a false call.

2.10.6 If caller line identification is operated, monitoring centres must not bar this facility on police calls.

## 2.11. ADMINISTRATIVE CHARGES

2.11.1 Each application for a URN both Intruder and HUA is subject to an administration fee payable by the system user. The URN fee is £43.49 plus VAT. Acceptable methods of payment (which may include BACS) are identified within Appendix A. The fee will be reviewed annually by NPCC. The current policy on charging is set out in Appendix E. URNs for vehicle tracking and lone worker services are dealt with in Appendices U & V of this document. Companies shall not misrepresent the cost of a URN to clients.

2.11.2 For intruder, HUA and CCTV systems the installation/maintenance company will, if requested, satisfy an invoice from the police for the payment of the URN administration fee on behalf of the system user who shall always remain responsible for the fee. The fee shall be the amount set out in the current edition of this document.

2.11.3 If the company satisfies an invoice referred to in 2.11.2, then the police and the company agree that this shall not constitute or imply any partnership, joint venture, agency, fiduciary or other relationship between either the company and the system user or the company and the police.

2.11.4 The fees for vehicle tracking and lone worker services will be reviewed annually and may be different from the intruder, HUA and CCTV system URN.

2.11.5 The administration fee charged by police forces must be clearly highlighted in writing to customers purchasing systems. Misrepresentation of the amount of the fee charged by the police will be deemed a fraudulent action and may result in legal action against the offending company.

2.11.6 Late payment of invoices may result in the suspension of the URN and the end user advised accordingly.

### 2.12 MEMORANDUM OF UNDERSTANDING

2.12.1 For non-compliance or poor performance including false activations caused by employees of a compliant company or monitoring centre, the procedure set out in the MOU should be implemented before suspension of URNs. (Appendix J).

## 3 OPERATIONAL TACTICS

### 3.1 POLICE ATTENDANCE - Type A Security Systems

3.1.1 For Type A security systems there are two levels of police response.

**LEVEL 1 – Immediate**
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 3 – Withdrawn**
No Police attendance, keyholder response only.

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

3.1.3 All new IAS and HUA applications will only qualify for a URN and police response if installed to the required standards. (See appendix F, Annexe C standards matrix).

3.1.4 Electronic Transfer of IAS and Hold up Alarms activations will be mandatory with effect from 1.4.2020.

### 3.2 INTRUDER ALARM SYSTEMS

3.2.1 IAS issued with a URN will receive LEVEL 1 response until three false calls have been received in a rolling 12 month period.

3.2.2 Following two false calls in a rolling 12 month period the customer will be advised, in writing, with a copy being forwarded to the maintaining alarm company informing them of the situation and recommending urgent remedial action.

3.2.3 Following three false calls in a rolling 12 month period LEVEL 3 will apply and police response will be withdrawn, not less than 14 days from the date of the Withdrawal letter. The customer will be advised in writing with a copy to the maintaining company,

who will be required to instruct the monitoring centre not to pass alarm activations to the police. Notification of withdrawal may also be sent to the monitoring centre.

3.2.4 Following withdrawal of response, the following conditions will apply in order to reinstate police response:

(i) Unconfirmed IAS will need to be upgraded to a confirmed DD243:2004 or BS8243:2010 standard. (All systems installed prior to DD243:2002 are designated unconfirmed).
*Where a system has been upgraded, a copy of the NSI Compliance/ SSAIB Conformity certificate will be required by the police.*

(ii) Confirmed DD243 (2002 / 2004) or BS8243:2010 systems will require the cause of the false alarms identified, remedial action taken and a period of 90 days free of false calls from the date of the last false activation (supported by evidence from the security company), unless an additional method of confirmation is installed.

**For further information see Appendix F –Annex C**

The security company should apply for reinstatement of response using **Annexe A of Appendix F.**

3.2.5 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. If the URN is for a combined system, only the element of the URN at level 3 will be deleted.

3.2.6 Representatives of the security industry will be consulted to assist in the monitoring of the effect of new technology and to make applicable recommendations to update these requirements and/or relevant codes of practice.

## 3.3 CCTV SYSTEMS

3.3.1 To enable remote detector activated CCTV systems to gain a URN for police response, systems are to be installed to the standards and requirements specified in **Appendix R**. False alarm withdrawal thresholds for CCTV systems are the same as IAS.

## 3.4 HOLD UP ALARMS

3.4.1 A deliberately operated device, known as a HUA, may be operated to summon urgent police assistance when a person is threatened with immediate personal violence or criminal act. 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.

3.4.2 Installation and reinstatement of HUA's must comply with the ten point plan as specified in **Annexe B** of Appendix F and **Appendix T**.

3.4.3 HUA's issued with a URN will receive LEVEL 1 response until two false calls have been received in a rolling 12 month period. Following the first false call the customer will be

advised in writing, with a copy being forwarded to the maintaining alarm company informing them of the situation and recommending urgent remedial action.

3.4.4 Following two false calls in 12 months LEVEL 3 will apply and police response will be withdrawn not less than 14 days from the date of withdrawal letter. The customer will be advised in writing with a copy to the maintaining company who will be required to instruct the monitoring centre not to pass alarm activations to the police. Notification of withdrawal may also be sent to the monitoring centre.

3.4.5 For restoration of HUAs which have lost response, confirmation is mandatory. Security companies should apply for reinstatement using **Annexe B** of Appendix F.
Note: With effect from 1.4.2018 telephone call back as a single method of confirmation will not be acceptable for reinstatement for systems installed in commercial premises.

3.4.6 Where mandatory confirmation is required, it will remain in force whilst the end user is in occupation.

**3.5 Combined IAS & HUA Systems**

3.5.1 In a system with both IAS and HUA, the remote signal shall differentiate between the two types.

3.5.2 Where the threshold for withdrawal of police response is reached the withdrawal will apply to the facility IAS or HUA which has reached the threshold. That part to which response has not been withdrawn continues to receive response until it reaches the withdrawal threshold in its own right.

**3.6 POLICE ATTENDANCE - <u>Type B Security Systems</u>**

3.6.1 The electronic security industry has seen an increase in the availability of Type B alarms. These are being sold and bought with the expectation of prompt police attendance. Whilst not wishing to preclude the ability to provide a prompt response to crimes in action, observations as to the development of this technology has led to significant amount of false calls and additional demands and higher expectations of police attendance than would be appropriate.

3.6.2 To obtain police attendance, Type B systems will require evidence from **a person at the scene** that a criminal offence is in progress which indicates that a police response is required. This will require the presence of a person(s) such as a member of public, owner or agent at or in close proximity to the location of the incident. The addition of electronic means or non-compliant systems to provide confirmation will not promote such systems to Type A to achieve police response.

3.6.3 There is no guarantee of police response to Type B systems. Type B calls should be passed to the police directly from a person at the location of the incident by dialling 101 or 999 as appropriate not through a third party or compliant/ non-compliant monitoring centre. The police response will depend on the quality of the evidence received and if given may be significantly slower to the response given to Type A systems.

3.6.4 Automatic dialling equipment **must not** be programmed to call police telephone numbers.

3.6.5 Calls received from non-compliant monitoring centres without a valid URN are **unlikely to** receive a police response.

3.6.6 Compliant ARCs must not pass Type B system activations via the police dedicated ex-directory telephone numbers.

## 4. LEARNING REQUIREMENTS

### 4.1 DATA PROTECTION ACT & GENERAL DATA PROTECTION REGULATION

4.1.1 The Data Protection Act 2018 and General Data Protection Regulation replace the Data Protection Act 1998 and place new obligations on organisations handling personal information.
Consequently companies that supply their clients personal information to Chief Officers of Police should ensure that they meet their obligations under the new legislation and in particular ensure that their clients are made aware that their information will be disclosed to the police and how it may be used by the police, including the fact that where the data is relevant to a complaint, it may be disclosed to the UKAS accredited inspectorate body recognised by the NPCC.

4.1.2 Information supplied must be accurate and kept up to date. Any alterations to the personal data supplied by security companies must be notified to the Chief Officer of Police within 28 days.

### 4.2 EUROPEAN COURT OF HUMAN RIGHTS CONSIDERATIONS

4.2.1 These requirements have been drafted taking into account the appropriate principles of the Human Rights Act 1998. It has also been subject to suitable legal vetting.

### 4.3 FREEDOM OF INFORMATION ACT 2000

4.3.1 The requirements for Police Response to Security Systems document is publicly available and published on the Secured by Design and NPCC website www.securedbydesign.com via the Security Systems requirements link or www.npcc.police.uk

4.3.2 Should any requests be received seeking further information about either this document, its implementation, procedures used by police forces or companies, or any other aspect, the request is to be dealt with by the force freedom of information officer or national referral unit.

### 4.4 RACIAL EQUALITY

4.4.1 These requirements have been drafted taking into account the appropriate principles of the Equality Act 2010

### 4.5 ADVERTISING

4.5.1 Installation Companies and monitoring centre's 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, or use a police force logo without the prior permission of the relevant Chief Officer of Police. Non-compliant companies and ARCs that are not registered with a police force to install/monitor Type "A" Remote Signalling Systems

must not imply to the public that they will receive Level 1police response to Type B security systems.

4.5.2 Companies that are registered with their local police force under the security systems requirements (Appendix "B") to install Type "A" remote signalling systems may use wording such as 'Police Compliant' and 'Meets Police Requirements'. Generic photographic material or images of police officers or vehicles may be used.

4.5.3 Advertising methods should not contain any references to recognised, registered or compliant lists held by individual police forces. The terms police approved, police preferred or working in conjunction with the police must **not** be used.

4.5.4 Companies engaged in telesales techniques should comply with the following:

- The supplier is not to make any representations of the product being approved, endorsed or authorised by the police force.
- The script reflects the above.
- Each supplier should comply with relevant legislation in relation to telesales/telemarketing.
- Each supplier should monitor sales staff, the content of sales calls, the identity and avoid any instances of high pressure selling e.g. through recording of calls.

4.5.4 Each supplier should be aware any complaints made to the police force regarding sales tactics may be re-directed to the relevant regulatory body for investigation.

**4.6 FINAL DISCRETION**

4.6.1 These requirements do not impose any liability on a police force, its officers or employees, or Police & Crime Commissioner arising out of any acts or omissions connected with the security system installation, including failure or timeliness in responding to any activations. 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

4.6.2 Issues which may require amendment must be forwarded to the Chair of the Security Systems Group, the address of whom may be obtained from the NPCC. The Chair meets with representatives of the British Security Industry Association (BSIA), UKAS accredited inspectorate bodies, the Fire and Security Association (FSA) the Insurance Industry, represented by the RISC Authority and other invited representative organisations to review such matters.

4.6.3 The Police Requirements and Response to Security Systems is the copyright of the NPCC. This document is available on the Secured by Design website www.securedbydesign.com via the Police Requirements and Response to Security Systems on the home page. This may be downloaded for individual use, but under no circumstances altered or amended.

4.6.4 Other documents referred to in the requirements (including the appendices) and communications on matters referred to within it must be in writing or electronic form. Electronic documents or copies of original documents shall be acceptable.

# 5 INDEX TO APPENDICES

## APPENDIX A

**VARIATIONS FORCE SERVICE STANDARD**

**(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 this document).**

**Force Logo, Chief Officer's name and headquarters address**

The Security Systems requirements have been adopted by the …… Police/Constabulary. The following variations permitted under the terms of this document 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 agreement (Appendix B).

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 security system companies must enclose a stamped addressed envelope with all correspondence requiring a reply.

*All correspondence should be addressed to the Supervisor, Alarms Administration Department, ……address.*

The Unique Reference Number (URN) remains the property of ……Police/Constabulary and must be quoted in all correspondence. In the interests of maintaining security of records, all enquiries concerning individual security systems must be made in writing or electronic means. Telephone enquiries regarding systems or particular alarm activations will not be accepted.

**APPENDIX B**

## APPLICATION TO BE ACCEPTED ON POLICE LIST OF COMPLIANT COMPANIES / POLICE REQUIREMENTS DOCUMENT

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

You must be registered with your Home Force where your main office/headquarters is situated **before** applying to other police forces for inclusion on their List of Compliant Security Companies.
Insert Name of Home Force registered with ……..……..……..……..

Legal Entity Name……..

Trading Name……..

Companies House Registration……..

Registered Office……..

……..

……..

……..

I have read the (*NAME OF FORCE) Constabulary Security Systems Requirements. 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)
Position in Company ……..……..

My company is inspected by…… for the following types of security

systems …… (Copy of certificate to be enclosed).

**This is a living document and may be subject to annual amendment. It is your responsibility to ensure that your company is aware of these amendments. The document is available on the Secured By Design website (www.securedbydesign.com).**

Signature.....

Title:-Mr/Mrs/Ms/Miss/other……..

Print Full Name.....

Date.....

Trading Address……

……Post Code……

Telephone Number ……

Email for correspondence ……

Email for invoicing ……

Our Alarm Receiving Centre(s)

(i) Name ……

Telephone Number ……(for police operational use)

(ii) Name ……

Telephone Number……(for police operational use)

NB * NAME OF FORCE refers to the constabulary to whom you are submitting this document.

**Please Return to:-**Alarms Administrator, (name of Force) Police Headquarters, Address

Data Protection Act 1998 and from May 2018 the Data Protection Act 2018 and the General Data Protection Regulation
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

This procedure should only be entered into with companies on the list of compliant security system installers and monitoring centres 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 (as amended by the Criminal Justice and Immigration Act 2008) applies and spent convictions, reprimands, warnings, cautions and conditional cautions (adult and youth) cannot be considered.

The intention is to curtail those with unspent 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. BS 7858 must be complied with, which includes references being 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, monitoring, administration, sub-contractors and any other role with access to security systems data (not fire systems) in accordance with BS7858 with a company on a force's list of “Compliant Security System 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 preferably 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.

(v) When a police check is required, the employer should then pass the request on to the alarms administration office of the police force area where the employee is based for work purposes. There should be no reason to carry out subsequent checks in other force areas.

(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 instigate checks and also advise employers where they consider an applicant meets/does not meet the criteria of these requirements.

(viii) **The police check will be limited to a PNC check against criminal convictions only**. The police will reply stating the person meets/does not meet the criteria of these requirements. Details of convictions will not be passed on to the employer.

(ix) In the event of a pending prosecution where the offence is relevant, a decision on suitability may be delayed subject to the outcome of the case.

(x) 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 initially 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.

(xi) These requirements only apply 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 police compliant list is subsequently identified as being unsuitable through his/her criminal convictions, police forces may notify the relevant employer that the subject does not meet the requirements. The subject of the report will be informed.

(xii) In the event of a request for a police check from a foreign national who has not been in continuous residence in the United Kingdom for the past 5 years the application will also require an attachment of the relevant Overseas Criminality Certificate/record check (OCC); this will need a form of authentication and be translated into English by a translation service that is a member of the Institute of Translation & Interpreting Companies or the Association of Translation Companies.

(xiii) In the event of a British Citizen having worked/resided outside of the UK for over a period of six continuous months in the last 5 years, they will also be required to provide an overseas criminal record check.

(xiv) In exceptional cases where a government body does not exist or is unable to supply an applicant with an OCC an applicant may be able to supply a sworn oath in place of an OCC.

**Useful Links:**

www.sia.homeoffice.gov.uk
Click on - Individual Licenses>Will I Pass the Criminality Check>Overseas Criminal Records Checks.
www.commissionerofoaths.co.uk

(xv) Any employer knowingly employing someone with an unspent criminal record that would otherwise preclude them from working within the alarms industry will be considered for removal from the police list of compliant companies.

(xvi) Employers must have policies in place to ensure that any company personnel subsequently found guilty of a criminal offence that would naturally preclude them from working within the alarms industry must disclose this fact to their employer immediately.

## CONVICTION CHECK PROCESS

### 1. New Alarm Company

Apply to force where the company's head office is based submitting Appendix C forms for all relevant employees.

Home force to carry out all conviction checks.

### 2. Existing Compliant Security Companies

Submit Appendix C checks for new staff as required as at (ii) above to home force.

**However**

If a compliant company has several different regional offices, then appendix C checks should be processed for staff that operate from the regional office by the force where that office is based. (This mainly applies to large national companies and prevents one force having to process all checks from national companies).

**APPENDIX C (continued)**

## FORM A – TO BE RETAINED BY THE POLICE

## REQUEST FOR A POLICE CHECK IN RESPECT OF AN APPLICATION FOR EMPLOYMENT WITHIN A SECURITY SYSTEM COMPANY

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 in assessing my suitability, spent convictions and cautions are not considered by the police. I authorise the police to inform my employer if they consider I meet/do not meet the criteria of their force requirements on security systems, because of any information obtained from police records. Where there is police bail or pending prosecutions the decision to notify my employer could be delayed for some considerable time.*

Surname……

All Forenames .....

Former Names .....

Title (Mr/Mrs/Ms/Miss/Other)……..

Date of Birth ...../...../..... Place of Birth .....

Nationality.....

If born outside of the United Kingdom
Date of residency in UK.....

Position in company .....

Present Address .....

.....

.....

Previous Addresses in last 5 years (give dates):

.....

.....

.....
(continue at the end of the form if necessary)

If you live overseas or you have spent six continuous months or more outside the UK, you must provide evidence of a criminal record check from the relevant country or countries. The checks need to cover the five years prior to this application.

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

Are you currently on the Sex Offenders Register
YES/NO

Are you about to be or are you currently the subject of a pending court case
YES/NO

Are you currently on police bail
YES/NO

**If YES**, to any of the above please provide details, including date(s), the offence, and the court or police force dealing.

I agree to notify my employer of any future relevant convictions
YES/NO

**Proof of identity is required**. Please produce one form of photo ID (e.g. passport or photocard driving licence) and one other form of ID, which must show your current address (e.g. most recent utility bill). If you do not possess a passport or photocard D/L then you must produce your birth certificate. Photocopies of the relevant pages of these documents must accompany this form.

Signature of applicant ..... Date .....

**Verification by Manager, Director or Company Secretary**
I certify that I have examined the above-mentioned original documents and confirm that they relate to the applicant.

Printed Name .....

Signature ..... Date .....

Position .....

## ADDITIONAL ADDRESS DETAILS

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

**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 Security Systems requirements. The particulars provided have been verified and I am satisfied they are accurate.

I confirm that Form B of Appendix C has been provided to the applicant.
I/We indemnify the Chief Officer of Police of (NAME OF FORCE) and all officers and police staff of the said police service against all actions, claims, costs and demands arising out of the giving of information in response to this request.

SIGNED ..... PRINT NAME .....

TITLE..... DATE .....

POSITION IN COMPANY .....

NAME AND ADDRESS OF COMPANY .....

.....

Address where employee is based, if different from above: .....

.....

---

PART C - For Police use only

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

- No trace of convictions on details supplied.
- The subject appears identical with the person whose criminal record is attached.
- The subject does not meet the requirements of this document.

SIGNED ..... DATE .....

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

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

**APPENDIX C (continued)**

**FORM B**

## DISCLOSURE OF CRIMINAL CONVICTIONS

## EMPLOYER TO HAND THIS FORM TO APPLICANT

### NOTICE TO THE APPLICANT

The Police, in applying the requirements on security systems, may preclude a company from its list of compliant security systems installers and monitoring centres 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 meet/do not meet the Security System requirements.

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 may advise an employer/ prospective employer that an individual does not meet the requirements, 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 (AS AMENDED BY THE CRIMINAL JUSTICE AND IMMIGRATION ACT 2008) APPLIES TO THIS REQUEST FOR INFORMATION. YOU ARE NOT REQUIRED TO DISCLOSE A CONVICTION WHICH HAS BECOME SPENT UNDER THE ACT.**

**APPENDIX D**

# Not in use

**APPENDIX E**

## ADMINISTRATION CHARGES

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 in **Appendix A**.

1. Each application for a URN or element of a URN is subject to an administration fee payable by the system user. The URN Fee is £43.49 plus VAT and will be reviewed annually by the Security Systems Group. (See Appendices U & V for vehicle tracking and lone worker systems URN charging).
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 or other payment method fails to clear or is not honoured, the URN will be cancelled and the security system company and the customer informed.
3. Where a system includes both intruder detection and HUA equipment, the administration fee will normally be payable for the issue of a URN for each element. This will be irrespective of whether forces issue separate or combined URN's. The fee will be applied as follows:

### New Systems

a) All new URN applications will attract the full fee for each element.

### Existing System Taken Over

a) Where a new occupier/owner/legal entity of premises takes over an existing security system with one element the full fee will be payable.

b) Where a new occupier/owner/legal entity of premises takes over an existing security system with both intruder and HUA elements a reduced fee of £65.23 plus VAT will be payable.

c) The same fee (as above) will be payable where an existing user decides to change their security company or a security company takes over an existing system.

(In above cases a, b & c the system retains false alarm history unless upgraded to DD243 2004 or BS 8243 2010)

Where a security company cancels a URN, a period of 28 days grace should be given to allow another security company (depending on the working practice of the force) to either takeover the existing or, apply for a new URN(s). Where a security company applies to takeover a URN from an existing company and/or maintenance contract, they may do so supported by the customer's authority. (Completion of a signed

Appendix G to include the name of previous maintainer and the new maintainer will suffice).

IF PAYMENT BY CHEQUE/POSTAL ORDER IS STILL REQUIRED BY FORCES, IT SHOULD BE MADE PAYABLE TO **YOUR LOCAL POLICE AND CRIME COMMISSIONER**. IT MUST BE ENCLOSED WITH THIS FORM AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY.

**APPENDIX E (Continued)**

4. The administration fee is not applicable when:

   a) A compliant security company acquires/purchases another compliant security company.

   b) A security company loses their inspectorate accreditation or ceases to trade and another company takes over the URNs within 90 days.

   c) Premises change of name or franchisee (Evidence will be required to ensure it is a change of name only and not change of owner/user/legal entity).

URN's will retain their false alarm history.

5. In the event of police forces and security companies failing to reach an agreement as to whether 3 or 4 above applies, the police security systems group secretariat should be consulted and will make recommendations to the respective force.

6. In the event that the installation does not proceed after the URN has been allocated, the fee is non-returnable.

7. All security system monitoring centres operating under these requirements must utilise the dedicated ex-directory lines nominated by each police force.

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

Note: If the company pays the URN fee on behalf of the customer referred to above, then the police and the company agree that this shall not constitute or imply any partnership, joint venture, agency fiduciary or other relationship between either the company and system user or the company and the police.

Requirements on Police Response to Security Systems (April 2018)

**Appendix F**

| | | | | | |
|---|---|---|---|---|---|
| **NOTICE OF:** | | | **INT URN** | **1** | |
| **VARIATION REASON(S):** | | **Installation Date:** | **HUA URN** | **2** | |
| | | **Variation Date:** | **URN** | **3** | |

| **NAME OF ALARM RECEIVING CENTRE** | **NAME OF INSTALLER** | **NAME OF MAINTAINER** |
|---|---|---|
| | | |
| Police Ref: | Police Ref: | Police Ref: |
| **Address** | **Address** | **Address** |
| | e-mail | e-mail |
| Tel: | Tel: | Tel: |

**DETAILS OF PROTECTED PREMISES**

| | | | | | |
|---|---|---|---|---|---|
| **HOUSEHOLDER** | **Title:** | | **Initial(s):** | | |
| | **Surname:** | | | | |
| | **Business Name:** | | | | |
| **Trading/signage/building/ other Name** | | | | | |
| **Description of building** | | | | | |
| **Address:** | | | | | |
| **Address:** | | | | | |
| **Town:** | | | | | |
| **County:** | | | | | |
| **Postcode:** | | Tel: | **(incl STD code)** | ( Protected premises) | |
| | | | **Mobile** | | |
| | | | **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** | |
|---|---|
| | |
| | |

| **GRADE OF SYSTEM** | |
|---|---|
| | |
| | |

| **STANDARD TO WHICH INSTALLED** |
|---|
| |

| **EXISTING URN NO.** | | | |
|---|---|---|---|
| IAS | | CCTV | |
| HUA | | Veh tracking | |

| **PREVIOUS USER (Company name when applicable)** |
|---|
| |

| **ADMIN FEE** | **SOUNDER DELAY** | |
|---|---|---|
| | | |
| | | |

| **CERTIFICATE /Contract no** | |
|---|---|

**Print name** .....

**Position** .....

.....

**Date:** .....

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



**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) | TYPE OF CONFIRMATION (1 2 3) | ADDITIONAL FEATURES (1 2 3) | Grade of System (1 2 3) |
|---|---|---|---|
| Intruder Alarm (IAS) | Audio | None | Grade 2 |
| Hold Up Alarm (HUA) | Visual | Smoke Generator | Grade 3 |
| Combined IAS/HUA | Sequential | CCTV | Grade 4 |
| CCTV | Audio and Sequential | Lighting | |
| Vehicle tracking | Visual and Sequential | Chemical trace | |
| Lone Worker | Visual and Audio | Access control | |
| CAT 5 | Visual, Audio and Sequential | Smoke Raid Control (HUA) | |

| ADMIN FEE (1 2 3) | STANDARD TO WHICH INSTALLED (1) | TYPE OF PREMISES (1) | VARIATION REASON(s) (1 2 3) |
|---|---|---|---|
| Applicable | BS 4737 | Retail | Upgrade to confirmation |
| Not Applicable | PD6662 2004 + DD243 2004 | Commercial | Signalling amendment |
| | PD6662 2010 + BS8243 | | New user |
| | PD6662 2017 + BS8243 | Public Sector | |
| | BS 4737 + DD: 243:2002 | Licensed | Change of user name |
| | BS 4737 + DD243 2004 | Domestic | Address amendment |
| **SOUNDER DELAY (1)** | BS 6799 Class VI | Industrial | Additional features |
| | BS 7042 | Bank or Financial | Takeover from another maintainer |
| | BS 8243 | | |
| 0 Minutes | BS 8418 2003 | Institutional | Change of Alarm Receiving Centre |
| 5 Minutes | BS 8418 2010 | Other | Maintenance contract cancelled |
| 10 Minutes | BS 8418 2015 | | |
| 15 Minutes | BS 8484 | | |
| | CAT 5 ATSVIVR | | System removed |
| | | | Change of sounder delay |

**APPENDIX F - ANNEXE A**

**April 2018**

## APPLICATION FOR RESTORATION OF POLICE RESPONSE TO AN INTRUDER ALARM

Following the withdrawal of response letter the security company is required to apply for reinstatement using this form. Remedial work and/or re-certification of the system may be required as detailed below.

N.B. With regards to Combined URNs withdrawal of response of the IAS will not affect the status of the HUA. Please note, however that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated will be deleted. It is therefore essential that you give this matter your urgent attention.

| URN | NAME & ADDRESS OF PREMISES | INSTALLER / MAINTAINER |
|---|---|---|
| | | |

The remedial work required will be dependent on the existing status of the system, as follows:

| CURRENT STATUS | REQUIREMENT | COMPLETED (√) |
|---|---|---|
| 1) Unconfirmed system | Upgrade to DD243:2004 or BS 8243 * | ☐ |
| 2) DD243 system pre 2002 | Upgrade to DD243:2004 or BS8243 * | ☐ |
| 3) DD243:2002/2004 or BS8243 | Identify cause, remedy, and detail remedial action in box below ** | ☐ |

* **Note there is no requirement to upgrade to PD6662 to regain police response.**

** 90 days clear of false calls from the date of the last false activation will be required unless an additional method of confirmation is installed.

Identify the cause of the 3 false alarms which led to the withdrawal and **give details of remedial work** carried out (supported by evidence, such as an engineer's report sheet)

| Date | Cause | Means of Reset *** | Remedial Work |
|---|---|---|---|
| **1.** | | | |
| **2.** | | | |
| **3.** | | | |

*** State whether reset by engineer or managed (remote) reset.

Where a system has been upgraded a copy of the new NSI or SSAIB certificate of compliance/conformity must be forwarded with this application.
The information I have given is true to the best of my knowledge and belief. False or misleading information could lead to the loss of the URN

Signed:……Name……Date:……

**Appendix F- ANNEXE B**

**April 2018**

## APPLICATION FOR RESTORATION OF POLICE RESPONSE TO A HOLD-UP ALARM

| URN | Name & Address of Premises | Installer/Maintainer |
|---|---|---|
| | | |

**Following the withdrawal of response letter the security company is required to apply for reinstatement using this form. Remedial work and/or re-certification of the system may be required as detailed below**
**Please note that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated to the HUA will be deleted. It is therefore essential that you give this matter your urgent attention.**

Please put a cross in the boxes below for YES

1. Is a police response still required? ☐

2. If the answer to the above question is no, have appropriate measures been put in place to ensure that signals are not passed to the police? (The user may need to consult with their insurance company if the device has been removed). ☐

3. Confirmation is mandatory – is this in place? **(See note 1)** ☐

Type of Confirmation (please cross as applicable) **(See note 2)**

a) Call-back for domestic/residential premises only ☐

b) Sequential ☐

c) Video ☐

d) Audio ☐

4. Has the system been clear of false calls for 90 days? **(See note 1)** ☐

5. Are all of the Hold-Up devices dual action? ☐

6. Has the Duress facility been removed? **(See note 3)** ☐

7. Has user training been given? ☐

8. Does the Hold-Up alarm comply with all other aspects of Appendix T 10-point plan? ☐

| Date | Cause | Remedy |
|---|---|---|
| 1. | | |
| 2. | | |

**I declare the End User(s) have been fully trained in the confirmation method and procedures to be followed in the event of the HUA being activated**.

The information I have given is true to the best of my knowledge and belief.

Signed .....

Date .....

Name ..... (please print)

Position in Company .....

**Note 1**

When a method of confirmation has been implemented or replaced, response may be reinstated to HUA's before the 90 day period.
Where confirmation is mandatory to regain police response, an assessment must be carried out by the security company, to ensure that an appropriate confirmation method is used. In considering call back, audio or visual intervention, the purchasing contractor or other person responsible for health and security under applicable legislation must ensure adequate support systems in place in the premises to ensure that no-one is placed at undue risk. Documentary evidence of this process must be retained by this person for inspection.
The method of confirmation used must be based on the security needs of the end user(s) and not for commercial reasons.

**Note 2**

Confirmation methods to comply with BS8243

**Note 3**

(Only BS EN 50131-1 Grade 4 (Grade 3 in exceptional circumstances) & BS 7042 systems are exempt from this requirement).

**Please note that false or deliberately misleading information provided on this form could lead to the loss of the URN.**

**APPENDIX F – ANNEXE C**

| **STANDARDS MATRIX** | | | |
|---|---|---|---|
| New Applications for Intruder and Hold Up Alarm(s) URN's | | | |
| System Status | Requirement | Fee Required | Action to be taken by the alarm company. |
| New Application for New System | PD6662:2010 or PD6662:2017 & BS8243:2010 | 1 Fee HUA<br>1 Fee IAS | Apply to Security Systems Office on App F with App G |
| New Application for Existing System with no Previous Police Response | PD6662:2004 & DD243:2004 or PD6662:2010 & BS8243:2010 | 1 Fee HUA<br>1 Fee IAS | Apply to Security Systems Office on App F with App G raise new certificate or copy of original installation cert. (Must be dated pre 1st June 2012) |
| Reinstatement of Intruder and Hold Up URNs | | | |
| IAS Level 3 (Unconfirmed systems) | DD243:2004 or BS8243:2010 | N | Apply to Security Systems Office on App F Annexe A |
| IAS Level 3 (Confirmed systems) | DD243:2002/2004 or BS8243:2010 90 Days Clear of false calls unless an additional method of confirmation is installed. | N | Apply to Security Systems Office on App F Annexe A |
| Unconfirmed HUA Level 3 | Method of HUA Confirmation Either Call-Back (Domestic only), Sequential, Video or Audio. (Discretionary 90 days clear of false calls) | N | Apply to Security Systems Office on App F Annexe B |
| HUA Level 3 (Hold Up Confirmation Failed) | Alternative Method of HUA Confirmation (Discretionary 90 Days clear of false calls) | N | Apply to Security Systems Office on App F Annexe B |

| Deletions | | | |
|---|---|---|---|
| IAS Deleted Poor Performance | PD6662:2004 & DD243:2004 or PD6662:2010 & BS8243:2010 + 90 Days Clear | 1 Fee IAS | Apply to Security Systems Office on App F with App G + copy of original installation cert + Annexe A detailing remedial work. |
| HUA Deleted Poor Performance | PD6662:2004 & DD243:2004 or PD6662:2010 & BS8243:2010 + 90 Days Clear + method of HUA confirmation | 1 Fee HUA | Apply to Security Systems Office on App F with App G + copy of original installation cert + Annexe B detailing remedial work. |
| Deleted By Alarm Co | PD6662:2004 & DD243:2004 or PD6662:2010 & BS8243:2010 | 1 Fee HUA<br>1 Fee IAS | Apply to Security Systems Office on App F with App G + copy of original installation cert. |

**APPENDIX G**

## HAZARDS AND SITE RISKS STATEMENT - HEALTH & SAFETY ACT

**(MUST BE COMPLETED BY OCCUPIER)**

Police officers will not normally enter the premises without the keyholder. However, this may be necessary on occasions due to suspicious circumstances. So officers may be pre-warned of site risks you are required to state any site hazards.

| | **Hazard details apply to the building(s) and grounds of these premises.** | | | | | | **Please tick:** | √ |
|---|---|---|---|---|---|---|---|---|
| POND | | BASEMENT | | DOGS | | | CONTAGIOUS SAMPLES | |
| SWIMMING POOL | | FRAGILE ROOF | | DANGEROUS ANIMALS | | | FLAMMABLE SUBSTANCES | |
| RIVER FRONTAGE | | DANGEROUS STRUCTURE | | FIREARMS/SHOTGUNS | | | FUEL STORAGE | |
| GLASS COPING WALLS | | LOW CEILING BEAMS | | AMMUNITIONS | | | CHEMICALS | |
| RAZOR WIRE | | SLIPPERY FLOORS | | EXPLOSIVES | | | RADIO ACTIVE MATERIALS | |
| INSPECTION PITS | | FURNACE | | DANGEROUS MACHINERY | | | ASBESTOS | |
| SETTLEMENT TANKS | | ELECTRICITY SUB-STATION | | GAS CYLINDERS | | | SPRINKLER SYSTEM | |
| VATS | | ATM INSIDE PREMISES | | TOXIC MATERIALS | | | NONE | |

| | **PLEASE STATE ANY ADDITIONAL SITE HAZARDS – ADDITIONAL FEATURES** |
|---|---|
| | |

**Should site circumstances change you must update our records.**

1. I am aware that there is a police Alarm Administration fee payable (£43.49 + VAT) on the issue of **each** Unique Reference Number.
2. If this form is being completed in preparation for a take-over of a URN from an existing company and/or maintenance contract, I hereby authorise that change

Signed (customer) ……..

Name ……

Address of protected premises……

……

……

**If this form is not completed correctly the Appendix F will be returned**

Signed ……

Name ……

Alarm Company ……

Position in Company ……

Date

**APPENDIX H**

## POLICE ADVICE TO MEMBERS OF THE PUBLIC SEEKING INFORMATION ON SECURITY COMPANIES

To obtain information on companies who supply and install security systems such as Intruder Alarms / Hold-Up Alarms / CCTV systems etc., within your locality, we advise you contact the following Independent Inspectorate Bodies who will furnish you with the relevant details (the police are not able to provide this information):-

NSI (National Security Inspectorate)
Sentinel House, 5 Reform Road, Maidenhead, Berkshire SL6 8BY
Tel: 01628 637512 Fax: 01628 773367 E-mail: nsi@nsi.org.uk
Website: www.nsi.org.uk

SSAIB (Security Systems & Alarm Inspection Board)
7-11 Earsdon Road, West Monkseaton, Whitley Bay, Tyne & Wear. NE25 9SX
Tel: 0191 296 3242 Fax: 0191 296 2667 E-mail: ssaib@ssaib.co.uk
Website: www.ssaib.org

Independent Inspectorates are not-for-profit approval bodies who carry out inspection services for the security industry and protect customer interests. They are governed by UKAS (United Kingdom Accreditation Service), the sole accreditation service recognised by the Government.

Please note - if you are also planning to invest in the type of security system that would receive police response to its alarm activations, then *only* security companies 'Approved' by an Independent Inspectorate Body *and* who are listed with the police force in your locality are permitted to offer this service.

Once you have obtained details from an Independent Inspectorate Body of 'approved' security companies, who install security systems in your locality to the required European/British Standards we advise the following :-

(a) Check the address and credentials of the company and proof of identify from their representative before disclosing personal security details

(b) Obtain written quotations from at least two 'approved' security companies.

(c) Ask if the security company representative can provide you with a list of police rules for occupiers of 'monitored' alarmed premises and also written confirmation that they are currently registered with the police force in your area for the transmission of alarm activations from new installations.

(d) Ensure that the quotation specifies that the installation will be to current European/British Standards for that relevant security system and that it includes the terms of maintenance and monitoring contracts.

(e) Ensure the company operate a 24-hour call-out service and emergency attendance within four hours.

(f) Check that the installation and security company is acceptable to your insurance company.

(g) Avoid long term monitoring contracts and only pay for one year in advance.

(h) Terms which transfer inappropriate risks to consumers may be unfair and the Office of Fair Trading (OFT) have suggested that one kind of risk that should not be unfairly imposed on the consumer is that of the suppliers own insolvency. This may occur where the purchase price of goods or services, or a large part of it, is demanded substantially earlier than is needed to cover the supplier's costs. Such a prepayment assists the cash flow of the supplier, but is liable to be lost to the consumer if the business is wound up before completion of the contract.

**PLEASE NOTE** - When investing in Security Systems for your home or business it is not advisable to deal with cold callers or telesales enquiries – you should avoid doing doorstep or telephone business. Many traders who call at your door are honest and genuine, however, some are not and can be extremely persuasive. Examples of bad practices associated with cold-calling and door-step selling include - pressure selling, waiving your rights to a cooling off period, unclear contracts, over priced security systems and unduly raising the fear of crime. If members of the public have serious doubts about the legality or sales techniques being employed by any security company they should contact their local police or Trading Standards for advice.

For further information on intruder alarm advice for domestic properties visit www.securedbydesign.com

For consumer rights visit www.gov.uk/consumer-protection-rights

Get help from Citizens Advice about your consumer rights. They can also refer your complaint to Trading Standards officers who may then investigate on your behalf.

**Citizens Advice**
0345 404 0506
0345 404 0505 (Welsh Language)

**APPENDIX I**

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

Dear Sir/Madam

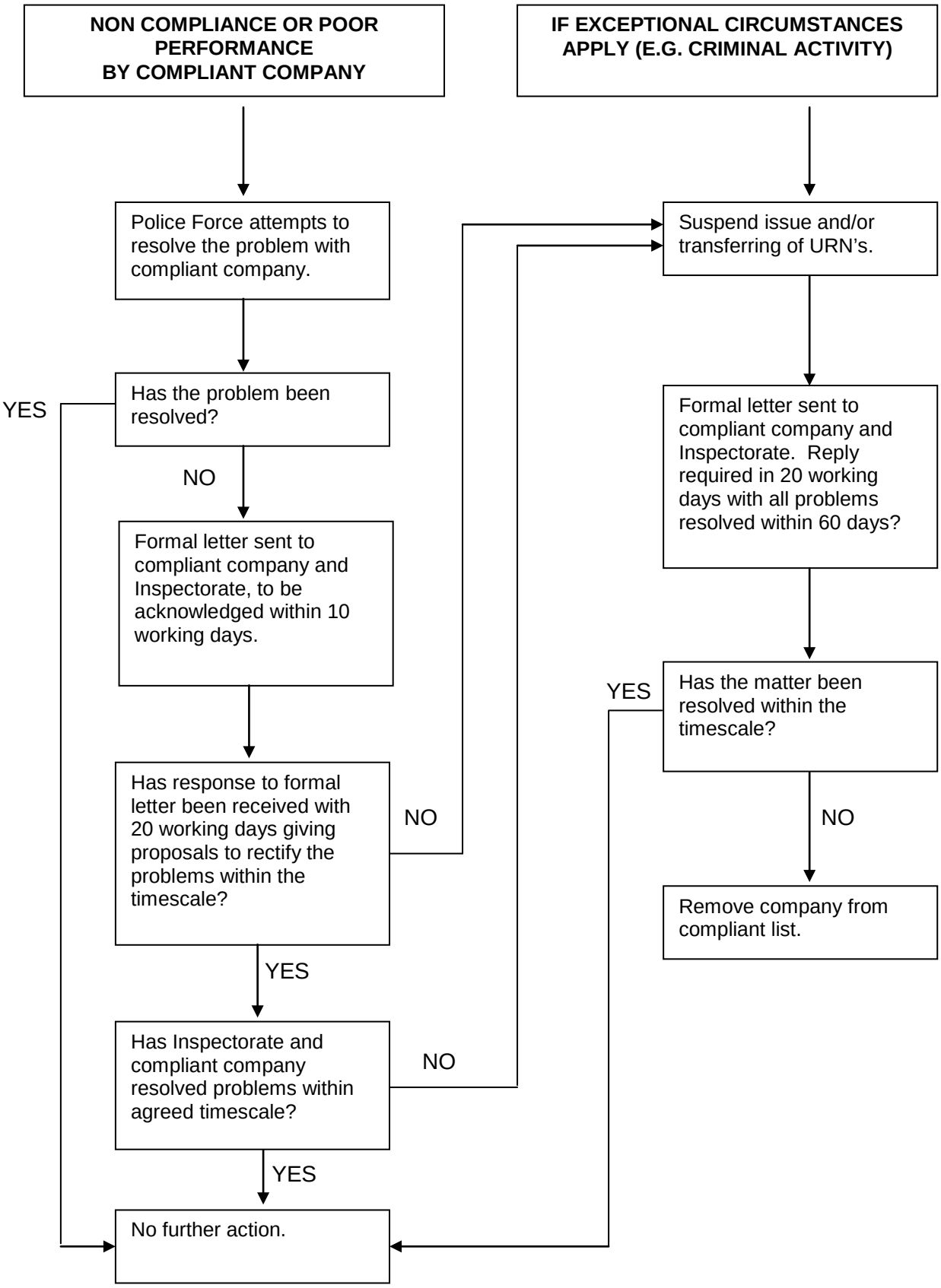
A properly installed security system will help to protect your premises when it is unoccupied. As you are considering the installation of a remote signalling security system you should be aware that the police have safeguards to reduce levels of false calls which divert us away from other tasks in your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

To avoid misunderstanding, here is a précis of the conditions. However, should you require further information please contact your local police alarms administration department.

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 a guarantee of the company's work. You should seek confirmation from the company that it is compliant with police requirements 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. Some 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 Clean Neighbourhood and Environmental Act 2005,may result in prosecution. Please check with the installing company, or your local authority for details.
6. Security systems will receive a police response determined by the nature of demand, priorities and resources which exist at the time. If an intruder alarm generates 2 false calls in a rolling 12 month period you will be advised in writing so that you may take remedial action. It is important that you take remedial action as failure to do so could result in loss of police response to the system.
7. Following 3 false calls in any rolling 12 month period on your Intruder Alarm police attendance will be withdrawn.
8. If your system has a separate Hold-Up Alarm police response will be withdrawn after 2 false calls in any rolling 12 month period.
9. Police attendance may be restored if remedial action has been taken to rectify the fault, or when the system has achieved 3 months free of false calls. The application must be submitted by your security company, with supporting evidence. It is therefore in your interest to identify and correct the cause of any false alarm in conjunction with your alarm company at the earliest opportunity.
10. 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.
11. 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.
12. In accordance with the Data Protection Act 2018 and the General Data Protection Regulations 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.

**APPENDIX J**

**MEMORANDUM OF UNDERSTANDING**



**APPENDIX K**

## POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION

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 to your system.

You are advised that police personnel may have to be withdrawn from the premises before the arrival of a keyholder. In this case the keyholder may contact the police and ask them to re-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 adopted the following requirements:

Every user having a system which produces two false calls within a rolling 12 month period, shall be served with a notice requiring action to be taken to prevent further false calls.

Should three (two for Hold Up) such calls be received within any rolling 12 month period, police response will be withdrawn. Response may be reinstated if remedial action has been taken to rectify the fault, or when the system has achieved three months free of false calls. In the event of restoration of response being delayed for more than 6 months, the URN will de deleted. If the URN is for a combined Intruder/Hold-Up Alarm, only the element that is off response will be withdrawn.

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.

Ensure that the maintaining alarm company or the alarm receiving centre is informed before commencement of any building or electrical work that may affect the operation of the intruder or hold-up system.

2. KEYHOLDERS

You should provide your alarm company with at least two keyholders for your premises. These keyholders shall be trained to operate the alarm, be contactable by telephone, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and able to attend the premises within a 20 minute period. A key safe product is not to be used as an alternative to a keyholder.

3. NOISE NUISANCE

Your attention is also drawn to the Control of Noise Order 1981, The Environmental Protection Act 1990 and the Clean Neighbourhood and Environment Act 2005. This includes a 20 minute limit on the operation of audible warning devices.

4. HOLD UP ALARMS (HUA)

The police requirements for security systems states “HUA’s may be operated to summon urgent police assistance when a person is threatened with immediate personal violence or criminal act”. However in many instances HUA’s are used where there is no threat to persons within a defined area. Without knowing the circumstances under which the HUA’s are activated, the police must respond. You should be aware that in the current policy, if you use the HUA twice within in a rolling twelve month period and there is no threat to persons in a defined area, you may lose police response for 90 days.

Accidental misuse happens when staff are not trained in the use of HUA's or visitors to the premises have access to the HUA and press it out of curiosity. It is important that the HUA is placed where members of the public cannot have access.

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

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

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

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

5. Data Protection Act and General Data Protection Regulation

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,

**APPENDIX L**

**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 could 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 standard PD 6662 (scheme for the implementation of European Standards) or BS 8418 and Codes of Practice identified in the police requirements 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 or in conjunction with your monitoring centre.

Yours faithfully,

**APPENDIX M**

## LETTER TO BE FORWARDED TO CUSTOMER 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 requirements governing the installation, maintenance, monitoring and use of security systems. The requirements include 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 rolling 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.

Regrettably, should you have a total of three false calls within a rolling twelve month period, it will be necessary to consider the withdrawal of police response to activations from your system, a situation we would wish to avoid.

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

**APPENDIX N**

## 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 your system has been upgraded if required, or remedial action has been taken to rectify the false calls and a period of 90 days free of false calls has been achieved. The action required will depend on which security system you currently have installed. Please contact your security company to clarify which option applies.

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 advise them of the contents of this letter as soon as possible.

In the event of restoration of response being delayed for more than 6 months, the system will be deleted from our files.

Yours faithfully,

Copy to: Security System Company

**APPENDIX O**

**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, has been made without prejudice on our part and should further false calls occur then police response could be withdrawn again as per the Police Security Systems Requirements.

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

Yours faithfully,

**APPENDIX P**

**DELETION OF UNIQUE REFERENCE NUMBER – LETTER TO CUSTOMER**

Dear Sir/Madam,

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

Response has remained withdrawn for a period in excess of 6 months without an application for reinstatement. As a result the decision has been made to delete the URN allocated to your system effect from 14 days from the date of this letter.

Your security company has been advised accordingly.

Yours faithfully,

**APPENDIX Q**

**DELETION OF UNIQUE REFERENCE NUMBER– LETTER TO SECURITY SYSTEM COMPANY**

Dear Sir/Madam,

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

Response has remained withdrawn for a period in excess of 6 months without an application for reinstatement. As a result the decision has been made to delete the URN allocated to your system effect from 14 days from the date of this letter.

After that time no further calls should be passed to the police. Your client has been advised accordingly.

Yours faithfully,

**Appendix R**

# 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 URNs from police forces.

1.2 Companies monitoring remotely monitored detector activated CCTV systems, known as RVRCs 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 these police requirements, will be known as Type A systems and will be issued with a URN.

1.4 Systems for which police attendance may be required and which operate outside the procedures identified in the police requirements, will be known as Type B systems. URNs 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 Police Security Systems Requirements 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:

- Police Security Systems Requirements
- BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice
- Relevant clauses of BS EN 62676-4 2015 as called up by BS8418

2.2 RVRCs monitoring detector activated CCTV systems will conform to all of the following standards:

- BS 5979 (CAT II) or BS8591:2014 (CAT II) or BS EN50518
- 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 2018 and General Data Protection Regulation 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 Security Systems Requirements. A URN will be issued in line with the relevant police force requirements (Appendix A of the NPCC Security Systems Requirements 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 and the requirements of the Data Protection Act 2018. The ICO CCTV Code of Practice (latest edition) and where applicable the government's Surveillance Camera Code of Practice.

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 there is criminal activity (or attempt) 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 RVRC's using digital recording methods will adhere to the procedures for processing digital images, issued jointly by the Home Office, Police and CAST.

## 5. MANAGEMENT INFORMATION

5.1 RVRC's will provide management information when required .

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 Security Systems Requirements (Clause 3 refers) for the relevant police forces in relation to the total number of incidents incorrectly passed to the police.

## 6. INDEMNITY

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

# National Police Chiefs' Council
# (ENGLAND, WALES AND NORTHERN IRELAND)

**Requirements for Security System Services**

I For the issue of a URN by police forces in England Wales and Northern Ireland, 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 BS EN ISO/IEC 17065:2012 by the 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.

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 Annexe 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 Annexe 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, in accordance with the Memorandum of Understanding (Appendix J).

k. Invite a member of the Security Systems Group to attend board meetings as an observer for agenda items relating to this scheme.

l. Be invited to the Security Systems Industry Liaison Group meetings and/or relevant meeting when deemed necessary by the NPCC.

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. Trade lawfully, ethically and comply with the Consumer Contracts Regulations Act 2013.

c. Should hold and maintain relevant insurance in respect of employers, public and product liability to include efficacy and wrongful advice.

Guidance – security companies should take advice from their insurance broker to determine the amount of cover needed based on the size of the company and the work they undertake.

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 security systems in accordance with the appropriate documents in Annex A.

f. Have adequate arrangements, documented procedures and systems in place for all of their activities.

Guidance – This covers all aspects of a company's installing, maintaining and monitoring activities and includes –

Personnel (includes vetting, competence, qualification)

Sales (includes enquiry, survey, quotation, order)

Installation (includes design planning, commissioning, and 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.

Complaint handling needs to show logging, corrective action and review procedures.

g. Have suitable premises where confidentiality can be maintained 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 Annex A.

h. Have the necessary resources to support all 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. Shall have sufficient business activity, relevant to the scope of this policy to enable competence and trading history to be determined by certification bodies.

j. Have immediate access to and comply with standards and documents identified in Annex A.

k. Have customer contracts describing the products and services to be supplied together with the associated terms and conditions.

l. 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.

m. Not engage in pressurised selling or unlawful trading practices. Companies shall comply with the Consumer Protection from Unfair Trading Regulations 2008.

n. Monitoring and maintenance contracts shall not exceed a period of three years and payments in advance shall not exceed one year.

IV New standards and documents applicable to this scheme will be notified by the secretary to the NPCC Security Systems Group to all certification bodies accredited to this scheme

V Where amendments to this scheme are deemed appropriate by the National Police Chiefs' Council a consultation meeting will be instigated for attendance by those concerned.

**British Standards and European Norms**
**(Current issue unless stated – see notes 1 & 2).**

| | |
|---|---|
| BS 4737 | Intruder Alarms in Buildings (mostly withdrawn see note 1) |
| BS 7042 | High Security (withdrawn see note 1) |
| BS 8418 | Remotely monitored detector activated CCTV Systems |
| BS 5979 | Alarm Receiving Centres (Category II) (Withdrawn see note 1) |
| BS 8591 | Alarm Receiving Centres (Category II) (not Intruder & Hold up Alarms). See Note 2 |
| BS 6799 | Wire free Alarms (withdrawn see note 1) |
| BS 62676-4 | Video surveillance systems for use in security applications – Part 4 Application Guidelines. |
| BS 7858 | Security screening of individuals employed in a security environment |
| PD 6662:2017 | Scheme for the application of European Standards for intruder and Hold-Up Alarm systems. |
| PD 6662:2010 | Scheme for the application of European Standards for intruder and Hold-Up Alarm systems. (Remains acceptable for new systems until 31st May 2019). |
| PD 6662:2004 | Scheme for the application of European Standards for intruder and Hold-Up Alarm systems (Withdrawn see note 1) |
| IA 1501:2015 | Industry agreement on PD6662:2010 |
| PD 6669:2017 | Guidance for the Provision of Alarm Transmission Systems (ATS) (Optional Standard – to be reviewed April 2019) |
| BS EN 50518 | Monitoring and Alarm Receiving Centres |
| BS EN 50131 | Series Intruder & Hold up Alarms |
| BS EN 50136 | Series Alarm Transmission systems |
| BS EN 50131-8 | Security Fog Devices (applies under PD6662) |
| BS 8473 | Management of False Alarms |
| BS 8243 | Installation & configuration of Intruder & HUAs designed to generate confirmed alarm systems (applies under PD6662) |

| | |
|---|---|
| BS 8484 | Provision of Lone Worker Device Services |
| BS 8593 | Code of Practice for the deployment and use of body worn video. |

**British Standards Institution Drafts for Development (Latest Issue)**

| | |
|---|---|
| BS DD 242 | High Security (withdrawn see note 1) |
| BS DD 243 | Applies under PD6662:2004 (Withdrawn see note 1) |
| BS DD 244 | Wire Free Alarms (withdrawn see note 1) |
| BS DD 263 | Alarms Systems Commissioning, Maintenance and remote support (applies Under PD6662) |
| BS 9263:2016 | Alarms Systems Commissioning, Maintenance and remote support (applies Under PD6662:2017) |
| DD CLC/TS 50131-7:2010 | Alarm Systems – Intrusion Systems – Application Guidelines |
| DD CLC/TS 50131-7:2008 | Applies under PD 6662:2010 (Withdrawn see note 1) |
| DD CLC/TS 50131-7:2003 | Applies under PD6662:2004 (Withdrawn see note 1) |

**Notes:**
Certain standards are in a period of “Dual running” with previous issues, and either current OR the previous issue may be acceptable for a specified, limited period.

1. Certain older and withdrawn standards or parts of standards are still included in this list for the benefit of legacy systems that remain in service.
2. BS 8591 is used in conjunction with BS EN 50518 series.
3. BS 7958 is called up by BS 8418 in relation to RVRCs

**Vehicle Tracking**
Category 5 Criteria for System Operating Centres June 2010
Category 5 Criteria for original Equipment Manufacturers
Centre for Applied Science & Technology (CAST) 14/02 Stolen Vehicle Tracking and Remote Immobilisation Systems
CEN TS 15213 series Road transport & traffic telematica – After-theft systems for recovery of stolen vehicles.

**Legislation**
The Clean Neighbourhood and Environment Act 2005 set out requirements for intruder alarms, keyholders and noise.
The Companies Act 1985, 1989 & 2006

## APPENDIX T

# TEN POINT PLAN FOR HOLD UP ALARMS

### 1) FILTERING

Monitoring centres are now in a position to filter unwanted false activations, with confirmation in place false calls will be reduced.

### 2) WITHDRAWAL OF POLICE RESPONSE

Police response will be withdrawn to the HUA part of the system after a maximum of 2 false calls in a rolling 12 month period.

Where a system loses response to a HUA, the security company should liaise with the end user to see if the Hold-Up element is necessary. If it is not required it should be removed.

When a form of confirmation has been implemented, police response may be reinstated to HUA's before the 90 day period. Any subsequent loss of response, after confirmation has been put in place, a system must have an alternative method of HUA confirmation and achieve 90 days free of false calls (discretionary) supported by evidence from the security company. (Appendix F Annexe C refers).

### 3) HUA DEVICES ON CIE OR ACE SHOULD BE SEGREGATED FROM THE MAIN KEYS, DEDICATED, DEFINED AND ARE 2 SEPARATE BUTTONS SYNCHRONISED PUSH.

### 4) HUA DEVICES ON CIE OR ACE SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

### 5) DURESS CODES SHOULD ONLY BE ALLOWED FOR BS 7042 OR BS EN 50131–1 GRADE 4 SYSTEMS

The logic of restricting duress codes to high security systems to ensure that the risk warrants the facility. Inadvertent use of the duress codes from the CIE can lead to a significant amount of false activations.

Individual applications to police forces for duress facility may be considered for Grade 3 systems if the following requirements are complied with:

1. In premises that require high security and duress has been identified as an essential requirement from the risk assessment.
2. Duress is notified separately from the hold-up alarm signal.
3. Duress should not be initiated by using a digital key (fob).

### 6) DURESS FACILITY SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

### 7) SINGLE ACTION 'SINGLE PUSH' HUA DEVICES ARE NOT PERMITTED

This has been standard in the industry for many years, systems must be upgraded to 'double push' HUA devices.

### 8) TIME DELAY DEVICES ARE NOT PERMITTED

In these types of systems the HUA is pressed once to start a timer. The occupier can then answer a door, check for intruders etc. If the HUA is not pressed a second time, the timer will time out and the HUA is sent.

### 9) PORTABLE HUA DEVICES (WIRELESS DEVICES) SHOULD BE DEDICATED AND NOT INCORPORATE ANY OTHER FUNCTION. THEY SHOULD HAVE 2 SEPARATE BUTTONS, SYNCHRONISE PUSH TO ACTIVATE

This requirement is to stop single button type HUA's, e.g. care alarm type systems being used for HUA's. This has been standard in the industry for many years, systems must be upgraded to 'double push' wireless devices.

## 10) TRAINING / RE-TRAINING OF USERS

The training or re-training of users must be incorporated into the handover/maintenance. The user should be responsible for the training of their keyholders and this must be documented within the maintenance report.

Documentation should be provided to indicate when to use and when not to use a HUA device. The keyholder must be made aware of the serious implications of misuse.

**APPENDIX U**

# REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING AFTER-THEFT SYSTEMS WITH VEHICLE IMMOBILISATION FOR VEHICLE RECOVERY

## 1. INTRODUCTION

1.1 This appendix sets out the police requirements for the installation and monitoring of After Theft Systems with Vehicle Immobilisation for Vehicle Recovery (ATSVIVR).

1.2 Only qualified and registered personnel who meet these police requirements can install ATSVIVR systems.

1.3 Systems Operating Centres (SOC's) who meet these police requirements can monitor ATSVIVR systems.

1.4 A SOC must agree and sign the NPCC and Industry approved indemnity letter and return this to each individual police force as part of the URN acceptance procedure.

1.5 A URN will be issued to a SOC for the purpose of monitoring ATSVIVR systems. This URN will be issued by each police force.

1.6 The police response to a reported ATSVIVR system which meets the requirements set out in this appendix will be level 1.

1.7 Other types of vehicle tracking systems that operate outside of this policy will be known as type B systems and a URN will not be issued to SOC to monitor such systems.

1.8 Any ARC's/SOC's who have existing vehicle tracking contracts known as legacy systems (no vehicle immobilisation) with the police may continue monitoring and reporting those existing systems, but these ARC's/SOC's will not be issued with a URN.

## 2. ATSVIVR REQUIREMENTS (See Annex A of Appendix U)

### 2.1 INSPECTORATE REQUIREMENTS

For an ATSVIVR system to be accepted by an SOC the installation service shall be inspected in accordance with the provision of this document by a certification body accredited to EN 17065 by the United Kingdom Accreditation Service. The exception to this is ATSVIVR systems fitted by the Original Equipment Manufacturer (OEM) at the car manufacturing plant.

For the SOC to be acceptable to NPCC it shall be inspected in accordance with the provisions of this document by a certification body accredited to EN 17065 with the scope of BS 5979 CAT II or BS 8591 CAT II or BS EN 50518 by the United Kingdom Accreditation Service.

### 2.2 SYSTEM INSTALLATION REQUIREMENTS

a. Installation shall be carried out by the car manufacturer at source or by a dealership or as an after-market fit to the ATSVIVR manufacturers' specifications.

b. The after-market fit shall only be undertaken by a company that is approved by an UKAS accredited inspectorate.

c. The ATSVIVR system installed shall meet the installer requirements set down in the CEN TS 15213 series (*Road transport and traffic telematics – After-theft systems for the recovery of stolen vehicles).*

### 2.3 COMMISSIONING REQUIREMENTS

a. The commissioning of the ATSVIVR will meet the requirements laid down in the Thatcham CAT 5 Criteria for After Market and OEM for System Operating Centres (SOC) monitoring after theft systems for vehicle recovery.

b. The commissioning shall be undertaken by organisations approved by Thatcham or a UKAS accredited inspectorate

### 2.4 MONITORING (SOC) REQUIREMENTS

The requirements of the SOC are:

a. BS 5979 CAT II or BS 8591CAT II or BS EN 50518

b. All personnel to be vetted to BS 7858

c. SOC parts of the CEN/TS 15213 Series

d. Home Office Centre for Applied Science and Technology (CAST) 14/02 – stolen vehicles

e. CAT 5 criteria as listed in Appendix S

## 3. LEGAL REQUIREMENTS

All documentation and data pertaining to personal data of the owner of the vehicle with an ATSVIVR system installed shall be processed as per the Data protection Act 2018 and General Data Protection Regulation.

## 4. POLICE ATTENDANCE

a. For ATSVIVR systems police attendance will be a level 1 – immediate/urgent.

b. If a single customer has 3 false alarm calls in a rolling 12 month period the SOC will remove that customer from police response until the customer can prove that the fault/procedure failures that caused the false alarms has been corrected. If the customer continues to have false alarms the customer will lose police response for 3 months and will only be reconnected if the 3-month period is free from false alarms.

c. No SOC URN can be withdrawn from response by an individual police force, but individual police forces can request through the security systems secretariat that the MoU is implemented on a poor performing SOC.

## 5. PROCEDURES

**5.1** When a vehicle is stolen the vehicle owner shall contact their local police and report the incident and obtain a crime reference number (CRN).

**5.2** The vehicle owner shall then contact the SOC and report the stolen vehicle and give the SOC the CRN.

**5.3** The SOC will then locate the stolen vehicle and contact the relevant police force.

**5.4** The SOC will keep in touch with the relevant police force directing the police to the location of the stolen vehicle.

**5.5** The SOC shall keep monitoring the location of the stolen vehicle until informed otherwise by the police.

**5.6** If required the SOC will activate the stolen vehicle's "immobilisation" device. It is important to note that the order to activate the vehicle's immobilisation device can only be given by a police officer who has the stolen vehicle in their line of sight.

## 6. MANAGEMENT INFORMATION

**6.1** The SOC will ensure that they have a false alarm management system in place.

**6.2** The SOC shall hold alarm statistics on all their customers and when required provide to NPCC relevant system management statistics.

**6.3** The SOC will inform customers who have repeated false alarms that they may loose police response if the cause of the false alarm is not remedied. The SOC will keep statistics on such cases.

## 7. URN REQUIREMENTS

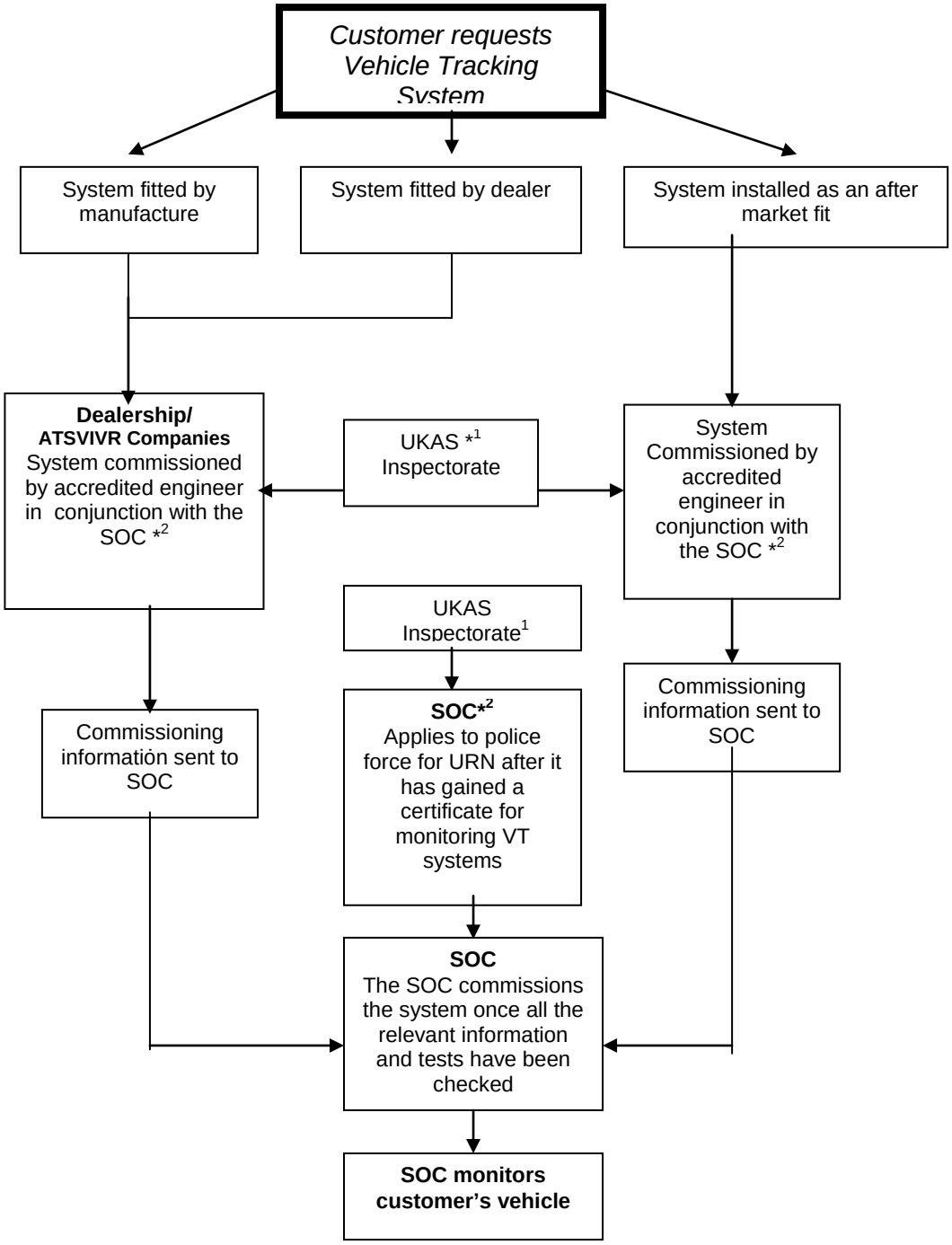
**7.1** The SOC will apply to the relevant police force area for a URN. The cost of the URN will be £52.55 plus VAT

**7.2** The SOC is to apply to the police alarm administrator for a URN using Appendix F of these requirements.

## 8. INDEMNITY

This document does not impose any liability on any police force, its officers or the police and crime commissioner arising out of the failure or timeliness in responding to activation from an ATSVIVR system.

NPCC VEHICLE TRACKING REQUIREMENTS FOR THE ALLOCATION OF A URN FOR A THATCHAM CATEGORY 5 SYSTEM WITH VEHICLE IMMOBILISATION CAPABILITY




Notes:

*1 Accredited engineer shall be vetted (BS 7858 and have a police or CRB check).

*2 The SOC is to submit the approved indemnity letter to police forces.

**APPENDIX U – ANNEX B**

## AFTER THEFT VEHICLE IMMOBILISATION SYSTEMS INDEMNITY DOCUMENT FOR SYSTEM OPERATING CENTRE

To: Chief Constable :……(Name of Force).

From

Date

Reference CAST 14/02 – STOLEN VEHICLE TRACKING NPCC AND HOME OFFICE GUIDANCE TO COMPANIES ON POLICE POLICY (Including After Theft Vehicle Immobilisation Systems)

The SOC operated by (**Name of Company**) is willing to indemnify you as stated in The HOSBD 14/02 Clause 9.1 which states:

> "Vehicle tracking and locator companies will indemnify, in writing, each chief constable where it is intended that the system will operate. The indemnity shall cover police forces, their officers and servants, the chief constable and all members of the police service, against any claim under any course of action made by any person in respect of any loss, damage, expense, personal injury (including death), wrongful arrest, prosecution or charge caused by the negligent operation of the system by the company, or by any malfunction of the system which results in a vehicle being wrongly identified as stolen".

It is important to note that the SOC will only operate the After Theft Vehicle Immobilisation System once they have been requested to do so by a police officer whose identity has been confirmed and who is in visual contact with the stolen vehicle and who has confirmed to the SOC that the stolen vehicle is parked in a safe place.

The SOC will not indemnify against:

a. The failure of the vehicle immobilisation system (hardware/software) once the command has been sent.

b. The failure of the communication network outside of the SOC control to send the signal to the target vehicle.

c. Any failure due to faulty immobilisation system installation into the vehicle.

d. Any delay of the activation of the immobilisation system, after the SOC has dispatched the signal, due to the geographical location of the vehicle and the time the network uses to transmit the signal from the SOC to the vehicle.

e. Any incident that occurs after the SOC has been requested by a police officer to activate the vehicle immobilising signal and the successful activation of the immobilising device.

The SOC believes that the above liability requirements place responsibility for liability on the SOC on the area that the SOC has control of and no other areas.

The SOC believes that the use of CAST 14/02 and the use of vehicle immobilisation systems will be a service of benefit to the police and that through a partnership approach can contribute to the reduction of vehicle crime in the UK.

Signature_____

Name of Person_____

Job Title_____

Date_____

**APPENDIX V**

# POLICE REQUIREMENTS FOR LONE WORKER SERVICES

## 1. INTRODUCTION

1.1 This appendix sets out the police requirements for the provision of lone worker services requiring police response.

1.2 Monitoring centres who meet these police requirements will be able to apply for a URN to gain police response for lone worker systems.

1.3 Monitoring centres shall have filtering and verification processes in place to cut out any false alarms from LWDs and the police shall only be called in situations where a police response is required. In non-threat situations other types of response from other agencies or supervisors may be required. In these circumstances the police should not be called otherwise it may count as a false activation.

1.4 The supplier shall inform the customer of the Security Systems Requirements including this appendix.

1.5 The customer shall be trained by the supplier to use the LWD and also how to cancel any false activations that occur so as to minimise any false calls.

## 2. URN REQUIREMENTS

2.1 The Monitoring Centre will apply to the relevant police force for a URN. The cost of the URN will depend on the number of devices monitored nationally:

- Under 10,000 £52.55 plus VAT per annum.
- 10,000 – 50,000 £78.82 plus VAT per annum.
- 50,000 or above £105.10 plus VAT per annum.

Renewable on 1st April per annum.

2.2 The monitoring centre is to apply to the police alarm administrator for a URN using the Appendix F of these requirements.

## 3. FALSE ALARMS

3.1 The amount of false alarms as stated in clause 3.2 & clause 3.4 of the main Security Systems Requirements does not apply to lone worker systems.

## 4. DEVICE AND SUPPLIER REQUIREMENTS

4.1 Lone Worker Devices shall meet the lone worker device requirements laid down in BS 8484.

4.2 Body Worn Video devices shall meet the BWV requirements laid down in BS 8593- Code of Practice for the deployment and use of body worn video.

4.3 Lone Worker Suppliers shall:

a. Meet the lone worker supplier requirements laid down in BS 8484

b. Meet the requirements as laid down in Appendix S, sub clause III, except sub clause 'I'

c. The supplier shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body to the provisions of the Police Requirements and Response to Security Systems document.

## 5. MONITORING CENTRE REQUIREMENTS

5.1 The monitoring centre shall:

a. Meet the requirements of BS 8484 and where applicable BS 8593

b. Conform to BS 5979 CAT II or BS 8591CAT II or BS50518

c. Be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of the requirements for lone worker systems.

**See Annexe A re monitoring centre operators advice.**

## 6. LEGAL REQUIREMENTS

All the documentation and data pertaining to personal data with respect to Lone Worker/Body Worn Video Services shall be processed in accordance with the the Data Protection Act 2018.

## 7. POLICE ATTENDANCE

7.1 Lone worker services which meet the requirements of the Security Systems Requirements will receive a LEVEL 1 – Immediate police response, (see 3.1.1 of this document).

7.2 If police response is withdrawn it will be for a period of 3 months, or until the customer can prove to the relevant police force that the cause of the false alarms has been corrected.

7.3 Police response will not be withdrawn by individual police forces without prior consultation with the security systems secretariat.

## 8. PROCEDURES

8.1 When a LWD is activated the monitoring centre shall carry out the procedures set down in BS 8484 and those set down in the response agreement, (note the response agreement does not supersede the police requirements).

8.2 The monitoring centre operator is to determine the nature of the incident from audio and video information received and where safe to do so, contact the lone worker either by 2 way radio or other means to find

out more about the incident to ensure the correct level of response is attained and that the police are not called to a non-emergency response.

8.3 Once the monitoring centre operator has determined that the incident does require an emergency police response the operator is to contact the police giving as much information about the incident as possible including the lone worker details and any information about other responders dispatched to the incident.

8.4 The operator is to update the police control room on any changes to the incident or lone worker location whilst the police are attending the incident.

8.5 The operator shall monitor the incident until informed otherwise by the police. The audio and video recordings of the incident may be required for police investigation and/or evidential purposes and should be managed as per the Data Protection Act.

## 9. MANAGEMENT INFORMATION

9.1 The monitoring centre and the supplier shall ensure that they have a false alarm management system in place.

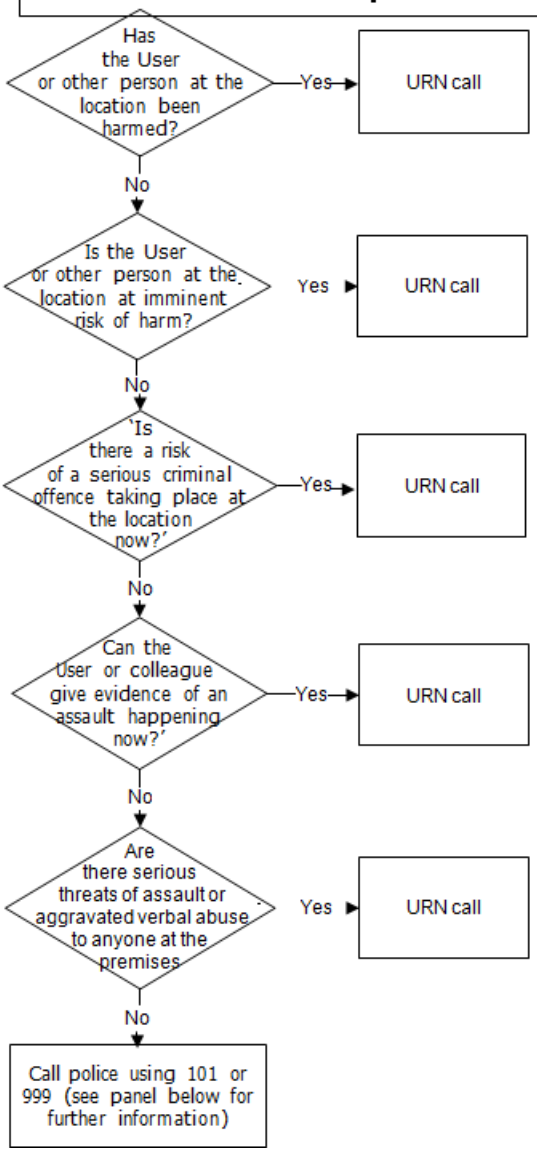
9.2 The monitoring centre shall hold statistics on all their customers and when required provide the police with relevant data.

9.3 The monitoring centre shall inform the customer when false alarms occur and when the customer is about to lose police response.

## 10. INDEMNITY

This document does not impose any liability on any police force, its officers or the police and crime commissioner arising out of the failure or timeliness in responding to an activation from a lone worker if the location information is not accurate.

# Use of a Lone Worker Device
## Advice to ARC operators on when, and when not, to use the URN




**This note gives guidance to ARC operators monitoring Lone Worker alarms**

In principle, the LW URN can be used in situations when there is risk to the Lone Worker, but not if there is no direct or indirect threat to the lone worker

It also gives information to suppliers and customers to clarify the difference between requesting police response from a Lone Worker device (LWD) and when a phone call to the police is more appropriate.

A 'fixed site' is defined as the customer's site where the LW does not normally leave the premises

All URN calls should have a confirmed location

Serious criminal offence at a fixed site **does** include:

- Serious threats being made to assault anyone at the site
- Threatening, abusive words or behaviour causing fear and distress to staff or members of the public, i.e. malicious/aggravated verbal abuse
- Such situations which may apply to others at the site and which may subsequently affect the Lone Worker

Serious criminal offence **does not** include non-emergency situations, including:

- Shoplifting (101)
- Disputes arising from customer complaints (101)
- Forecourt drive offs (101)
- Noisy parties in hotel rooms (101)

(See panel below for an expanded list and which number to call in such situations)

Note: Part 2 below

**For non-URN situations**

Use the following services to contact police
Fixed site situations: Use 101 for:

- Shoplifting
- Drive-offs/bilking
- Noisy parties
- Drug taking
- Criminal offence (any) already occurred
- Minor disorder/anti/social behaviour in the premises

External situations: Use 999 for:

- Public Order outside of premises
- Criminal offence in progress outside of premises

**Contacting the Police when using the URN system**

The ARC Controller should say:

- "This is a Lone Worker Personal Attack Alarm URN XXXX

And give the following information:

- The accurate location
- The reason for the event being policed
- That an assault has/is being committed or that serious threats and abuse have been heard on audio/reported by user and the user is in fear of being assaulted
- Maintain audio contact with the User
- Inform police if there are changes to the situation, e.g. Weapons are involved or the situation is downgraded

Note: Do not use the terms Amber or Red Alert as they mean nothing to police operators