



Police Operational Advice and Security Industry Requirements for Response to Security Systems

The National Police Chiefs' Council (NPCC) has agreed to these revised requirements 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 Serena Kennedy
Force/Organisation:	Merseyside Police
NPCC Business Area:	Prevention Co-ordinating Committee
APP/Reference Material	Reference Material
Contact details:	0151 777 8015
Review date:	April 2023

These revised requirements have been produced and approved by the NPCC Prevention Co-ordinating Lead. 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.

Summary of Amendments to previous document **National Police Chiefs' Council (NPCC) Police Requirements & Response to Security Systems**

Note	Formatting of spelling, capitalization, numbering, dates and similar standardized throughout the document. Header throughout document changed to '(May 2022)'
Title Page	Author – 'CC Steve Watson' changed to 'CC Serena Kennedy' Force/Organisation – 'South Yorkshire Police' changed to 'Merseyside Police' NPCC Crime Business Area – 'Crime Reduction' changed to 'Crime Prevention Co-ordinating Committee' Contact Details – '0191 375 2265' changed to '0151 777 8015' Review date changed to 'April 2023' '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' removed Copyright changed to '© August 2022 – NPCC'
Contents	Changed to reflect alterations to page numbering
2.1	(title) '(COMPLIANT)' inserted
2.1.3	'Alarm activations should be passed via the ECHO hub. Where a force is not ECHO ready then...' inserted
2.1.4	(a) '...Cat II and' changed to '... Cat II with the exception of clauses 8.3 and 9.2.'
2.2	(title) '(NON-COMPLIANT)' inserted
2.3.2	(d) now 2.3.3 (a) (e) now 2.3.3 (b)
2.3.3	Additional point - 'Police Compliant companies:' and Note added
2.3.3	(b) "...a procedure for..." changed to "...procedures and guidance..."
2.6.1	'To find correct police force...' changed to 'To find the correct police force...'
2.6.3	'...installation; the...' changed to '...installation. The...' and 'The URN is issued and owned by the police.' in bold
2.7.1	'...details and any change...' changed to '...details inclusive of any change...'
2.7.3	'...practicable.' changed to '... practicable and no later than 6 months after the date of transfer.'
2.8.4	'...will result...' changed to '...may result...'
2.8.6	'...keyholder or if there...' changed to '...keyholder if there...'
2.10.1	'...filter out false calls...' changed to '...filter out and manage false calls...'
2.11.1	'£45.66' changed to '£48.00'
3.1	(title) '(COMPLIANT)' added
3.1.1	"...police response is ultimately..." changed to "...police response will normally be immediate but is ultimately..." and "...and, therefore, cannot be guaranteed." added
3.1.2	'The police service has adopted the use of confirmed alarm technology as part of the effort to reduce false calls.' removed
3.1.3	now 3.1.2
3.1.4	now 3.1.3 and '...will be mandatory with effect from 1 st April 2020 where forces are...' changed to '...from compliant ARCs certificated to BS 5979 Cat II and BS EN 50518 became mandatory with effect from 1 st April 2021 where forces were...' and final sentence replaced with new guidance
3.2.3	'NB. It may be advantageous for police forces to send notification to ARCs.' added
3.3.1	'...to the standards and...' changed to '...to the standard BS8418 and...'
3.4.1	(1 st bullet point) '...petrol.' changed to '...fuel.'
3.4.4	(note) 'Since 1 st April 2018...' removed and '...has not been accepted...' changed to '...will not be accepted...'
3.6	(title) '(NON-COMPLIANT)' added
3.6.3	new point inserted
3.6.3 & 3.6.4	now 3.6.4 and '...audible only...' removed and '...monitored...' removed and '...from a person at the location...' changed to '...from the person at the scene...'
3.6.5	now 3.6.6
3.6.6	now 3.6.5
4.1.1	'...replace the Data Protection Act 1998 and place...' changed to '...replaced the Data Protection Act 1998 and places...' and '...should ensure that they meet their obligations under the new legislation and in particular ensure that their clients...' changed to '...should ensure they meet their obligations under current legislation and in particular ensure their clients...' and '...the fact that where...' changed to '...the fact where...'
4.1.2	2 nd sentence in bold
4.1.3	'It is incumbent upon police forces...' changed to 'It is the responsibility of each police force...'

4.2.1	"Note..." removed
4.4	"RACIAL EQUALITY" replaced by new point "OCCUPIERS LIABILITY ACT 1957"
4.5.1	"...police force logo..." changed to "...police force or NPCC logo..." and "...Chief Officer of Police." changed to "...Chief Officer of Police or Chair of the NPCC." and "...use the fear of crime..." changed to "...unduly use the fear of crime..."
4.5.3	'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 a police response to Type B systems.' changed to 'Non-compliant companies and ARCs must not imply to the public that they will receive an automatic police response.'
4.5.5	3 rd point '...(see Appendix S III.m).' added
5	Appendix D title changed to "CONVICTION CHECK GUIDANCE"
Appendices	All changed from '(April 2021)' to '(April 2022)'
Appendix B	Trading Address field '(as appears on Inspectorate Certificate see App S IIIg) added
Appendix A	'The NPCC Security Systems Requirements are available on the Secured by Design (SBD) website: www.policesecuritysystems.com ' added
Appendix C	3 rd paragraph "See Appendix D for clarification"
Appendix C	PROCEDURE (ii) '...', which includes references being required and taken up in the case of all new appointments, with...' removed and '...unexplained gaps in employment being satisfactorily accounted for.' replaced with 'Any unexplained gaps in employment must be satisfactorily accounted for.'
Appendix C	PROCEDURE (viii) new point inserted
Appendix C	PROCEDURE (viii) now (ix)
Appendix C	PROCEDURE (ix) now (x)
Appendix C	PROCEDURE (x) now (xi)
Appendix C	PROCEDURE (xi) now (xii)
Appendix C	PROCEDURE (xii) now (xiii)
Appendix C	PROCEDURE (xiii) now (xiv)
Appendix C	PROCEDURE (xiv) now (xv)
Appendix C	PROCEDURE (xv) now (xvi)
Appendix C	PROCEDURE (xvi) now (xvii)
Appendix C	PROCEDURE (xvii) now (xviii)
Appendix C	Form A (part a) (note to previous addresses) 'If you live overseas...' changed to 'If you live outside the UK...'
Appendix C	Form A (part a) (Signature of Applicant) 'NB: Typed or electronic signature is not acceptable' replaced with 'NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.'
Appendix C	Form A (part a) 'Verification by Manager, Director or Company Secretary' changed to 'Verification by Manager, Director, Company Secretary or HR Agent' and 'NB: Typed or electronic signature is not acceptable' replaced with 'NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.'
Appendix C	Form A (part B) 'NB: Typed or electronic signature is not acceptable' replaced with 'NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.'
Appendix C	Form A (part C) 3 rd option 'A decision on suitability cannot be made at this time' added to table
Appendix C	Form B "...Section 16, Theft Act 1968." changed to "...Section 3, Fraud Act 2006."
Appendix D	"CONVICTION CHECK GUIDANCE" created
Appendix E	(1) '£45.66' changed to '£48.00'
Appendix E	(3b) '£68.50' changed to '£72.00'
Appendix E	(4a) '...and takes over the URNs within 90 days.' added
Appendix E	(4b) 'A security company loses their inspectorate accreditation or ceases to trade and another company takes over the URNs within 90 days.' replaced with 'A security company no longer holds accreditation with an inspectorate body (as per 1.3 in the Preface of this document) and another compliant company takes over the URNs within 90 days.'
Appendix E	(4c) now (4e)
Appendix E	(4c) and (4d) new points inserted
Appendix F	(Application) 'what3words' box added below 'Or Other Type' box and 'O/S Grid Map Ref' box moved down one line
Appendix F	Annexe A under Note '** 90 days clear of false calls...' changed to '90 days clear of confirmed false alarms...'
Appendix F	Annexe B (3b) '****' added and under Note: new point added
Appendix F	Annexe C IAS Level 3 (Confirmed Systems) '...false calls' changed to '...confirmed false alarms...' and IAS Deleted '...of confirmed false alarms' added and HUA Deleted '...of false calls' added
Appendix G	'So officers may be pre-warned of site risks you are required to state any site hazards.' replaced by 'To ensure the safety of officers, the force must be pre-warned of site risks, therefore you are required to state any site hazards in accordance with the Occupiers Liability Act 1957.' and Other Site Hazard box reduced in size and (point 1) '...that there is a police alarm...' changed to '...', where applicable, there

will be a police alarm...' **and** (point 1) '£45.66' changed to '£48.00' **and** 'Business name of premises' field inserted **and** 'Customer email address' field inserted **and** '*' added to Customer Signature field and '* NB: Typed signatures will not be accepted. Secure electronic or wet signatures are acceptable.' Added

- Appendix S (III(m)) points (i) & (ii) added
- Appendix S (IV) '...secretary to the NPCC...' changed to '...secretary of the NPCC...'
- Appendix S Annexe A – Cyber Security Guidance Point 3 added **and** Cyber Security Guidance Notes - numbering and note 2 removed
- Appendix V (2.1) '...using Appendix F of these requirements.' added to first sentence **and** '£55.17' changed to '£58.00' **and** '£82.76' changed to '£87.00' **and** '£110.35' changed to '£116.00' **and** 'Renewable on 1st April per annum' removed
- Appendix V (2.2) 'The monitoring centre is to apply to the police alarm administrator for a URN using Appendix F of these requirements.' changed to 'Lone worker URNs are renewable annually on the 1st April. The monitoring centre is to advise the police alarm administrator of renewal requirements.'
- Appendix V (5.1(b)) 'BS 8591' changed to 'BS 9518'
- Appendix V (8.2) '...non-emergency response.' changed to '...non-emergency incident.'

Contents



Section	Page
1. Preface	6
2. Requirements and Procedure	6
3. Operational Tactics	11
4. Learning Requirements	14
5. List of Appendices	17
Appendix A	19
Appendix B	20
Appendix C	21
Form A	24
Form B	27
Annexe A	28
Annexe B	29
Annexe C	30
Appendix D	31
Appendix E	32
Appendix F	34
Annexe A	37
Annexe B	38
Annexe C	40
Appendix G	42
Appendix H	43
Appendix I	45
Appendix J	46
Appendix K	47
Appendix L	49
Appendix M	50
Appendix N	51
Appendix O	52
Appendix P	53
Appendix Q	54
Appendix R	55
Appendix S	57
Annexe A	60
Appendix T	62
Appendix U	(not in use)
Appendix V	64
Annexe A	66

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 the police response which is to be expected to an electronic security system as identified in the NPCC 'Requirements for Security Systems'.
- 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 requirements by individual forces are listed within **Appendix A** of this document.
- 1.5 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.

2. **REQUIREMENTS AND PROCEDURES**

2.1 **TYPE A (COMPLIANT) - REMOTE SIGNALLING SYSTEMS**

- 2.1.1 Systems should be monitored by Alarm Receiving Centres (ARCs), Remote Video Response Centres (RVRC) and Security Operations Centres (SOC). All centres must comply with BS 5979 (Cat II), or BS EN 50518 and BS 8591 (where required).
- 2.1.2 Unique reference numbers (URNs) will be issued by police forces for systems monitored by these recognised centres.
- 2.1.3 Alarm activations should be passed via the ECHO hub. Where a force is not ECHO ready, then all security system monitoring centres operating under these requirements must utilise the dedicated ex-directory lines nominated by each police force.
- 2.1.4 ARCs dealing solely with alarm systems within their own company premises (in-house monitoring), also known as Security Operations Centres, are exempt from the BS 5979 Cat II or BS EN 50158 Cat I certification provided:
 - a) The facility was operational with police consent prior to 31st October 1995, and there has been no change of premises **or** the ARC complies with BS EN 50518 Cat II with the exception of clauses 8.3 and 9.2.
 - 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 the NPCC Requirements Document.

2.2 TYPE B (NON-COMPLIANT) - SECURITY SYSTEMS & MONITORING CENTRES

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 for security systems which operate outside procedures identified at Section 2.1.

2.3. LIST OF COMPLIANT COMPANIES INSTALLING AND MONITORING 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, monitoring or administration of security systems, persons with criminal convictions (other than spent convictions). **Appendix C** sets out procedures and guidance for the implementation of this requirement.
- (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.

2.3.3 Police Compliant companies:

- (a) Once accepted will take responsibility for ensuring the company updates itself with amendments to this document, which is reviewed annually.
- (b) 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.
- (c) Compliant companies must not sub-contract or use a non-compliant company to install or maintain a security system.

Failure to comply with 2.3.3 may result in the company being suspended for 90 days, following which compliance may be removed. Point (c) above may also result in the deletion of the URN.

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** on the NPCC website.

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 the correct police force for application purposes go to www.police.uk, Find A Police Force 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.
- 2.6.4 Facilities for inspection of the installation shall be made available if required by the police service.
- 2.6.5 Address details of police force alarm administration units can be found at www.policesecuritysystems.com

2.7 VARIATIONS / TRANSFERS 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 inclusive of any change in maintainer and monitoring centre, in the form of **Appendix F and G**.
- 2.7.2 Transfers involving fewer than 10 premises to be submitted to the relevant force in the form of **Appendix F and G**.
- 2.7.3 Transfers involving 10 or more premises may, subject to individual force requirements, be submitted on a spreadsheet to the relevant force but **Appendix G** forms for each site will still be required. It will be the responsibility of the new maintenance company to submit the completed **Appendix G Hazard & Risk** forms as soon as practicable and no later than 6 months after the date of transfer.

Failure to comply could lead to the Memorandum of Understanding (MOU) being implemented and/or the URN being deleted.

2.8 KEYHOLDERS

- 2.8.1 All premises with Type A Systems shall have at least 2 keyholders, details of whom will be maintained by the monitoring centre. 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 (SIA) Licensing Regulations and BS 7984-1 in relation to keyholding and response.

NB: If the SIA regulations impede the commercial keyholding company from attending within 20 minutes of being notified, alternative keyholders must be registered in order to meet compliance with keyholder requirements at 2.8.1 and 2.8.2 above.

2.8.4 Failure of keyholders to attend when requested on 2 occasions in a rolling 12 month period may result in the withdrawal of police response for a 3 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.

2.8.6 Due to operational demands, responding officers may not always be able to remain at the premises and wait for the keyholder if there is no obvious sign of a criminal offence.

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 and manage false calls. This should be done in accordance with BS 8473. 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 Hold Up Alarm (HUA)/lone worker 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 when there has been no apparent damage, entry to the premises or 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, Intruder, HUA and CCTV system, is subject to an administration fee payable by the system user. The URN fee is £48.00 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 lone worker services are dealt with in **Appendix 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 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.
- 2.11.7 Non-payment of invoices may result in the deletion 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 Memorandum of Understanding (MOU) should be implemented before suspension of URNs. (**Appendix J**).

3 OPERATIONAL TACTICS

3.1 POLICE ATTENDANCE - TYPE A SECURITY SYSTEMS (COMPLIANT)

- 3.1.1 For Type A security systems there are 2 levels of police response.

LEVEL 1 – Immediate

It should be noted that police response will normally be immediate but is ultimately determined by the nature of demand, priorities and resources which exist at the time a request for police response is received and, therefore, cannot be guaranteed.

LEVEL 3 – Withdrawn

No police attendance, keyholder response only.

- 3.1.2 All new Intruder Alarm System (IAS), HUA and CCTV system applications will only qualify for a URN and police response if installed to the required standards. (See **Appendix F, Annexe C** standards matrix).
- 3.1.3 Electronic Transfer of IAS and HUA activations from compliant ARCs certificated to BS 5979 Cat II and BS EN 50518 Cat I became mandatory with effect from 1st April 2021 where forces were able to accept such activations. Once a police force has declared their 'Go-Live' date for ECHO connections, all ARCs will have 3 months from that date to become ECHO-connected to the force in question. ARCs failing to become ECHO-connected within the time frame will no longer be considered police compliant.

3.2 INTRUDER ALARM SYSTEMS

- 3.2.1 IAS issued with a URN will receive LEVEL 1 response until 3 false calls have been received in a rolling 12 month period.
- 3.2.2 Following 2 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 3 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.

NB. It may be advantageous for police forces to send notification to ARCs.

- 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 current BS 8243 standard. (All systems installed prior to DD243:2002 are designated unconfirmed).

Where a system has been upgraded, a copy of the National Security Inspectorate (NSI) Compliance/Security Systems & Alarm Inspection Board (SSAIB) Conformity certificate will be required by the police.

- (ii) Confirmed DD243 (2002/2004) or BS 8243 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 –Annexe 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.

3.3 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 standard BS8418 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 or is in fear of 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 unless the call is made with good intent. Misuse to summon police attendance to non-essential incidents may result in LEVEL 3 response.

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 fuel.
- 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.

- 3.4.2 HUAs issued with a URN will receive LEVEL 1 response until 2 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.

3.4.3 Following 2 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.

3.4.4 For restoration of HUAs which have lost response, confirmation is mandatory. Security companies should apply for reinstatement using **Annexe B** of **Appendix F** and the 10 point plan as specified in **Appendix T**.

Note: telephone call-back as a single method of confirmation will not be accepted for reinstatement for systems installed in commercial premises.

3.4.5 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 2 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 - TYPE B SECURITY SYSTEMS (NON-COMPLIANT)

3.6.1 There is no guarantee of police response to Type B systems. The processing and response time for Type B systems will be significantly slower than that for Type A systems. The police response, if provided, will depend on the quality of the evidence received.

3.6.2 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 amounts of false calls and additional demands and higher expectations of police attendance than would be appropriate.

3.6.3 ARCs monitoring Type B systems should pass activations for keyholder response only.

3.6.4 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. Type B system calls should be passed to the police directly from the person at the scene of the incident by dialling 101 or 999 as appropriate, **not** through a third party or compliant/non-compliant monitoring centre.

3.6.5 Compliant ARCs must not pass Type B system activations via the police dedicated ex-

directory telephone numbers.

- 3.6.6 Automatic dialling equipment **must not** be programmed to call police 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 (GDPR) replaced the Data Protection Act 1998 and places obligations on organisations handling personal information.

Consequently companies that supply their clients personal information to Chief Officers of Police should ensure they meet their obligations under current legislation and in particular ensure 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 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.**

- 4.1.3 It is the responsibility of each police force to ensure the data they hold is accurate and kept up-to-date by regularly conducting audits of alarm company records with no more than 2 years between audits.

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 website: www.policesecuritysystems.com via the Site Map and Group Initiatives
- 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 OCCUPIERS LIABILITY ACT 1957

- 4.4.1 The Occupiers Liability Act 1957 imposes a common duty of care on **occupiers** to lawful visitors. By virtue of s.1(3)(a), the Act applies not only to land and buildings but also extends to fixed and movable structures, including any vessel, vehicle or aircraft. See Appendix G Hazard & Site Risks

4.5 ADVERTISING

- 4.5.1 Installation companies and monitoring centres 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 or NPCC logo without the prior permission of the relevant Chief Officer of Police or Chair of the NPCC. Nor should they unduly use the fear of crime in order to sell 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 Non-compliant companies and ARCs **must not** imply to the public that they will receive an automatic police response.
- 4.5.4 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.
- 4.5.5 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 (see Appendix S III.m).
 - Each supplier should monitor sales staff, the content of sales calls, the identity of the recipient of the call and avoid any instances of high pressure selling e.g. through recording of calls.
- 4.5.6 Each supplier should be aware that 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.
 - (d) suspend/remove a company from the force compliant list.
- 4.6.2 Where a police force suspends or removes a company from their compliant list, consideration should be made by the NPCC Security Systems Group (SSG) as to whether this suspension or removal should be applied nationally.
- 4.6.3 Issues which may require amendment must be forwarded to the Chair of the SSG, 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.

- 4.6.4 The **Police Operational Advice and Security Industry Requirements for Response to Security Systems** is the copyright of the NPCC. This document is available at www.policesecuritysystems.com This may be downloaded for individual use, but under no circumstances be altered or amended.

5. INDEX TO APPENDICES

APPENDIX A	VARIATIONS FORCE SERVICE STANDARD
APPENDIX B	APPLICATION FOR INCLUSION ON POLICE LIST OF COMPLIANT COMPANIES/POLICE REQUIREMENTS DOCUMENT
APPENDIX C	DISCLOSURE OF CONVICTIONS
ANNEXE A	LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – MEETS REQUIREMENTS
ANNEXE B	LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – DOES NOT MEET REQUIREMENTS
ANNEXE C	LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – UNABLE TO PROCESS
APPENDIX D	CONVICTION CHECK GUIDANCE
APPENDIX E	ADMINISTRATION CHARGES
APPENDIX F	COMBINED NOTICE OF INTENTION TO INSTALL AND VARIATION FORM KEY TO COMPLETION OF APPENDIX F
ANNEXE A	APPLICATION FOR RESTORATION OF RESPONSE TO INTRUDER ALARM
ANNEXE B	APPLICATION FOR RESTORATION OF RESPONSE TO HOLD UP ALARM
ANNEXE C	STANDARDS MATRIX FOR NEW APPLICATIONS
APPENDIX G	HAZARDS AND SITE RISKS STATEMENT (HEALTH & SAFETY ACT)
APPENDIX H	POLICE ADVICE TO MEMBERS OF THE PUBLIC SEEKING INFORMATION ON SECURITY COMPANIES
APPENDIX I	LETTER TO BE HANDED TO POTENTIAL CUSTOMERS BY ALL COMPANIES INSTALLING SECURITY SYSTEMS
APPENDIX J	MEMORANDUM OF UNDERSTANDING
<u>APPENDICES K-Q ARE ADVISORY STANDARD TEMPLATES - FOR USE BY FORCES, IF REQUIRED</u>	
APPENDIX K	POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION
APPENDIX L	NOTICE OF URN TO INSTALLER
APPENDIX M	LETTER TO BE FORWARDED TO CUSTOMER AT 2 FALSE CALLS
APPENDIX N	LETTER FROM POLICE TO CUSTOMER ADVISING WITHDRAWAL OF RESPONSE
APPENDIX O	LETTER TO SECURITY SYSTEM COMPANY RE REINSTATEMENT OF POLICE RESPONSE
APPENDIX P	LETTER TO CUSTOMER ADVISING DELETION OF URN
APPENDIX Q	LETTER TO SECURITY SYSTEM COMPANY RE DELETION OF URN
APPENDIX R	REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS
APPENDIX S	NPCC - REQUIREMENTS FOR SECURITY SYSTEMS SERVICES

ANNEXE A	BRITISH STANDARDS AND EUROPEAN NORMS
APPENDIX T	TEN POINT PLAN FOR HOLD UP ALARMS
APPENDIX U	NOT IN USE
APPENDIX V	POLICE REQUIREMENTS FOR LONE WORKER SERVICES
ANNEXE A	USE OF LONE WORKER DEVICE - ADVICE

APPENDIX A (April 2022)

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).

(insert Force Logo, Chief Officer's name and headquarters address)

The Security Systems Requirements have been adopted by the *(force name)* Constabulary/ Police. 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 *(name of force)* Constabulary/Police Service Standard is to aim to attend all urgent calls within 10 minutes in the following areas *(insert areas)* and *(insert town names)* 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 *(force name)* Constabulary/Police 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.

The NPCC Security Systems Requirements are available on the Secured by Design (SBD) website: www.policesecuritysystems.com

APPENDIX B (April 2022)**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.

Name of Home Force	
Legal Entity Name	
Trading Name	
Companies House No.	
Registered Office	

I have read the (*) 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 (*) Police or being included on the (*) Police list of compliant companies.

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

Position in Company

My company is inspected by..... for the following types of security system.....

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

(*) Enter name of Home Force

(**) Enter name of company

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. This document is available on the Secured By Design website (www.policesecuritysystems.com).

Signature		Date	
Print Full Name		Title	
Trading Address (as appears on the Inspectorate Certificate see App S IIIg)			
Postcode		Telephone No	
Email (for correspondence)			
Email (for invoicing)			

Alarm Receiving Centre(s)

1	Name	
	Telephone	(for police operational use)
2	Name	
	Telephone	(for police operational use)

Please Return to: Alarms Administrator, (name of force & 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 (April 2022)

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. See **Appendix D** for clarification.

PROCEDURE

- (i) 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.
- (ii) Police checks must not take the place of normal recruitment procedures. BS 7858 must be complied with. Any unexplained gaps in employment must be satisfactorily accounted for.
- (iii) 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 BS 7858 with a company on a force's list of "Compliant Security Companies", or a prospective company wishing to go on the list, will be required to complete a form. The form will be consistent with the model layout as shown at Form A. This will be done after selection, **but before appointment**.
- (iv) 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.
- (v) 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.
- (vi) 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.
- (vii) 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.
- (viii) If a compliant security company outsources their HR functions they will be required to:

- a) Notify the relevant police force in writing authorising the force to accept documentation from the HR supplier
- b) Ensure that the HR supplier submits the correct documentation

Note: Appendix C results will be returned directly to the security company and not to the outsourced HR company.

- (ix) All applicants must give written permission for the police to instigate checks and also for the police to advise employers where they consider an applicant meets/does not meet the criteria of these requirements.
- (x) **The police check will be limited to a PNC check against criminal convictions only.** The police will reply using standard letter **Appendix C Annexe A** stating the person meets/does not meet the criteria of these requirements. Details of convictions **will not** be passed on to the employer.
- (xi) 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. The police will reply using standard letter **Appendix C Annexe B** stating a decision on suitability cannot be made at this time.
- (xii) 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.
- (xiii) 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 should be informed by the employer.
- (xiv) 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.
- (xv) 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.
- (xvi) 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.
- (xvii) 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.

- (xviii) 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.

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

CONVICTION CHECK PROCESS

1. New Security 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 Company

Submit **Appendix C** checks for new staff as required as at (iii) 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).

3. Police Scotland Companies

For companies in Scotland that wish to be compliant in England and Wales they are to apply to either Lancashire or Northumbria Police Forces. They should submit Appendix B requesting compliance and Appendix C checks for the relevant staff.

For companies in Scotland that are already compliant in England Wales they should only submit Appendix C checks for new members of staff, to either Lancashire or Northumbria Police Forces.

For companies in Scotland who wish to be compliant with PSNI Appendix B & Appendix C checks should be submitted direct to PSNI.

APPENDIX C (contd) (April 2022)

FORM A – REQUEST FOR A POLICE CONVICTION CHECK

(To be retained by the police)

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

I am aware that this employment is subject to a police conviction 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 the NPCC Security Systems Requirements document because of any information obtained from police conviction records. Where there is bail or pending prosecutions the decision to notify my employer could be delayed for some considerable time.

Surname		Title	
All Forenames			
Former Names			
Date of Birth		Place of Birth	
Nationality			
Date of UK Residency (if born outside United Kingdom)			
Position in Company			

Present Address		Postcode	
-----------------	--	----------	--

Previous addresses in last 5 years (give dates):

Between Dates	Previous Addresses (continue on additional sheet if necessary)		
		Postcode	
		Postcode	
		Postcode	

Note: if you live outside the UK or you have spent 6 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 5 years prior to this application.

1	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?	YES / NO
2	Are you currently on the Sex Offenders Register?	YES / NO
3	Are you about to be or are you currently the subject of a pending court case?	YES / NO
4	Are you currently on bail or under investigation for a criminal offence?	YES / NO

Note: if the answer is YES to question 3 or 4 and the offence is relevant, this request WILL be delayed pending the outcome of the investigation or court case.

I AGREE TO NOTIFY MY EMPLOYER OF ANY FUTURE RELEVANT CONVICTIONS.

Proof of identity

2 forms of ID are required:

1. Photo ID (e.g. passport or photo-card driving licence).
2. Another form of ID, which must show your current address and be dated within the last 3 months (not a driving licence).

If you do not possess a passport or photo-card driving licence then you must produce your birth certificate. Photocopies of the relevant pages of these documents must accompany this form.

Signature of Applicant		Date	
------------------------	--	------	--

NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.

Verification by Manager, Director, Company Secretary or HR agent

I certify that I have examined the above-mentioned original documents and confirm that they relate to the applicant.

Signature		Date	
Print Name			
Position in Company			

NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.

PART B - to be completed by the employer

The person identified above satisfies the conditions for requesting a police conviction 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		Date	
Print Name		Title	
Position in Company			
Company Name			
Company Address			
		Postcode	
Address where employee is based (if different from above)			
		Postcode	

NB: A typed signature will not be accepted. A secure electronic or a wet signature is acceptable.

PART C – for police use only

PNC records only have been checked against the above details:

Tick the relevant option:

No trace of convictions on details supplied		(✓)
The subject appears identical with the person whose criminal conviction record is attached:	The record meets the requirements of this document	
	The record does not meet the requirements of this document	
	A decision on suitability cannot be made at this time	

Signature		Date	
------------------	--	-------------	--

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

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

APPENDIX C (contd) (April 2022)

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 prohibit 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 3, Fraud Act 2006.

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. Failure to meet these requirements may affect the conditions of your employment.

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 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 C – ANNEXE A (April 2022)

LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – MEETS REQUIREMENTS

Dear Sir/Madam

Re: Request for name check – (name of applicant)

I refer to your request for a conviction check to be carried out in respect of the above named individual who is seeking employment with your Company.

The name of (name of applicant) has now been checked on the Police National Computer and I am able to confirm that this applicant appears to meet the requirements of the NPCC Requirements & Response to Security Systems Policy and that your employment of them would not conflict with Clause 2.3.2(b).

NB: THIS IS NOT A FORMAL POLICE VETTING PROCEDURE. IT SHOULD NOT REPLACE THE NEED FOR A DISCLOSURE AND BARRING SERVICE CHECK AND HAS NO CORRELATION TO ANY POLICE VETTING OR NATIONAL SECURITY VETTING PROCESS. IT IS SOLELY ISSUED FOR THE PURPOSES OF SECURITY SYSTEMS ADMINISTRATION.

Yours faithfully

APPENDIX C – ANNEXE B (April 2022)

LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – DOES NOT MEET REQUIREMENTS

Dear Sir/Madam

Re: Request for name check – (name of applicant)

I refer to your request for a conviction check to be carried out in respect of the above named individual who is seeking employment with your Company.

The name of (name of applicant) has now been checked on the Police National Computer and I am able to confirm that this applicant does not meet the requirements of the NPCC Requirements & Response to Security Systems Policy and that your employment of them would conflict with Clause 2.3.2(b).

NB: THIS IS NOT A FORMAL POLICE VETTING PROCEDURE. IT SHOULD NOT REPLACE THE NEED FOR A DISCLOSURE AND BARRING SERVICE CHECK AND HAS NO CORRELATION TO ANY POLICE VETTING OR NATIONAL SECURITY VETTING PROCESS. IT IS SOLELY ISSUED FOR THE PURPOSES OF SECURITY SYSTEMS ADMINISTRATION.

Yours faithfully

APPENDIX C – ANNEXE C (April 2022)

LETTER FROM POLICE TO SECURITY SYSTEM COMPANY RE RESULT OF APPENDIX C CHECK – UNABLE TO PROCESS

Dear Sir/Madam

Re: Request for name check – (name of applicant)

I refer to your request for a conviction check to be carried out in respect of the above named individual who is seeking employment with your Company.

Regarding the positive response to questions 3 and/or 4 on Appendix C Form A. We are not in a position to be able to process this application at this time, please re-submit the application once the circumstances have changed.

Yours faithfully

APPENDIX D

CONVICTION CHECK GUIDANCE

It must be emphasised that **Appendix C** deals with conviction checks only; they are not NPPV checks as referred to in the College of Policing Vetting APP (Approved Professional Practice) nor are they to be confused with Enforced Subject Access Checks.

To avoid persons of dishonest or violent background from gaining access to premises and security information, it is considered that the convictions should be relevant to protecting the security of the customer. For example, theft, burglary, dishonesty, supplying of drugs, offences of indecency and serious assault would certainly be relevant, but drink/drive convictions, minor public order and minor offences of assault would not, unless they were related to property crime. Juvenile convictions also require consideration as to their relevance and the current age of the applicant.

Cautions are an admission of guilt **but not** convictions. Non-conviction information may only be disclosed on the authority of an officer of NPCC rank. Alarms administration units must establish procedures for managing this process and any appeals arising from rejected applications.

Fixed Penalty Notices (FPN) are not convictions and, whilst they appear on a person's PNC record, they do not appear on the printed list of convictions.

Criminal Behaviour Orders (CBO) can be applied for by the police, councils and some other organisations. Chief Officers may need to be made aware of the circumstances causing the issue of a CBO and may wish to take this into account in deciding the applicant's suitability.

APPENDIX E (April 2022)

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 £48.00 plus VAT and will be reviewed annually by the Security Systems Group. (See **Appendix V** for 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 intruder detection, HUA equipment and CCTV system, 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 more than one element a reduced fee of £72.00 plus VAT will be payable.
- c) Any further URNs allocated at the same site/premises will be treated as a separate entity and fees as at a) and b) above will apply
- d) 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 & d the system retains false alarm history. This may be reconsidered upon appeal.

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 take over the existing, or apply for a new, URN(s). Where a security company applies to take over 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** 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 **APPENDIX G** AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY.

4. The administration fee is not applicable when:
- a) A compliant security company acquires/purchases another compliant security company and takes over the URNs within 90 days.
 - b) A security company no longer holds accreditation with an inspectorate body (as per 1.3 in the Preface of this document) and another compliant company takes over the URNs within 90 days.
 - c) A security company ceases to trade and another compliant company takes over the URNs within 90 days.
 - d) A security company becomes non-compliant with a police force and another compliant company takes over the URNs within 90 days.
 - e) 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).

In all above circumstances 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 SSG 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.

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.

NB: If the company pays the URN fee on behalf of the customer referred to above, 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.

APPLICATION TO INSTALL OR VARY A SECURITY SYSTEM

Appendix F (April 2022)

NOTICE OF:	Choose an item.	INT URN	1
VARIATION REASON(S)	Choose an item.	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	
Email		Email		Email	
Tel		Tel		Tel	

DETAILS OF PROTECTED PREMISES					
Householder Surname		Inits		Title	
Business Name					
Trading/Signage/Building/Other Name					

Address (1)					
Address (2)					
Town/City					
County					
Postcode		Tel at premises		(include dialling code)	
		Mobile			
		Email			

Type of Premises	Choose an item.				
Or Other Type					
what3words		O/S Grid Map Ref			
Directions from main road (include if rural / new site etc.)					

IF THIS FORM IS NOT COMPLETED AS APPROPRIATE, OR THE HAZARD AND SITE RISK STATEMENT IS NOT ENCLOSED, IT WILL BE RETURNED UNPROCESSED

TYPE OF SYSTEM	
Choose an item.	
TYPE OF CONFIRMATION	
Choose an item.	
ADDITIONAL FEATURE(S)	
Choose an item.	
Choose an item.	
Choose an item.	
GRADE OF SYSTEM	
Choose an item.	
STANDARD TO WHICH INSTALLED	
Choose an item.	
EXISTING URN	
IAS	
HUA	
CCTV	
PREVIOUS USER (company name if applicable)	
ADMIN FEE	SOUNDER DELAY
Choose an item.	Choose an item.
CONTRACT NUMBER	
PRINT NAME	
POSITION	
DATE	

Appendix F (lists)

KEY TO COMPLETION OF APPENDIX F	
<p>Select option 1, 2 or 3 in the 'Notice of' field, then select the appropriate data from the following lists. i.e. If number 1 is selected, complete all the fields marked (1) below.</p> <p>nb. If number 3 is selected, complete all the fields relevant to the variation.</p>	
NOTICE OF	<ol style="list-style-type: none"> 1. Application for a Unique Reference Number (URN) 2. Application to reinstate a Unique Reference Number (URN) 3. Variation to an existing security system
VARIATION REASON(S) (1 2 3)	Upgrade to Confirmation Signalling Amendment New User Change of User Name Address Amendment Additional Features Takeover from Another Maintainer Change of Alarm Receiving Centre Cancellation of URN System Removed
TYPE OF PREMISES (1)	Retail Commercial Public Sector Licensed Domestic Industrial Bank / Financial Institutional Other
TYPE OF SYSTEM (1)	Intruder Alarm (IAS) Hold Up Alarm (HUA) Combined IAS/HUA CCTV Lone Worker
TYPE OF CONFIRMATION (1 2 3)	Audio Visual Sequential Audio & Sequential Visual & Sequential Visual & Audio Visual, Audio & Sequential
ADDITIONAL FEATURES (1 2 3)	None Fog (Intruder) CCTV Lighting Chemical Trace Access Control Fog (HUA)
GRADE OF SYSTEM (1 2 3)	Grade 2 Grade 3 Grade 4
STANDARD TO WHICH INSTALLED (1)	BS 4737 PD6662 2004 + DD243 2004 PD6662 2010 + BS 8243 PD6662 2017 + BS 8243 BS 4737 + DD243 2002 BS 4737 + DD243 2004

	BS 6799 Class VI BS 7042 BS 8243 BS 8418 BS 8484 Secured By Design Standard
ADMIN FEE (1 2 3)	Applicable Not Applicable
SOUNDER DELAY (1)	0 Minutes 5 Minutes 10 Minutes 15 Minutes

APPENDIX F - ANNEXE A (April 2022)

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.

NB: 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.

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	✓ if completed
1	Unconfirmed system	Upgrade to DD243:2004 or BS 8243*	
2	DD243 system pre 2002	Upgrade to DD243:2004 or BS 8243*	
3	DD243:2002/2004 or BS 8243	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 confirmed false alarms 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

Signature		Date	
Print Name			

APPENDIX F - ANNEXE B (April 2022)

APPLICATION FOR RESTORATION OF POLICE RESPONSE TO A HOLD-UP 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.

NB: Please note that if this situation has not been satisfactorily resolved within 6 months, the URN allocated to the HUA will be deleted. It is therefore essential that you give this matter your urgent attention.

URN	
Name & Address of Premises	
Installer/Maintainer	

Select as relevant:

(✓)

1	Is this 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?*	
	(Identify type of confirmation by selecting a, b, c or d)**	
	a) Call back for domestic/residential premises only	
	b) Sequential (for definition see BS 8243 2010 clause 5.4.1.1)****	
	c) Video	
	d) Audio	
4	Has the system been clear of false calls for 90 days?*	
5	Are all the HUA devices dual action?	
6	Has the Duress facility been removed?***	
7	Has user training been given?	
8	Does the HUA comply with all other aspects of Appendix T (10-point plan)?	

Note:

*	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.
**	Confirmation methods to comply with BS 8243
***	Only BS EN 50131-1 Grade 4 (Grade 3 in exceptional circumstances) & BS 7042 systems are exempt from this requirement
****	Evidence may be requested that sequential confirmation is in place. This should be in the form of an ARC report with the unconfirmed and confirmed HUA signals highlighted

	Date	Cause	Remedial Work
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.

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

Signature		Date	
Print Name			
Position in Company			

APPENDIX F – ANNEXE C (April 2022)

STANDARDS MATRIX

New Applications for Intruder and Hold-Up Alarm(s) URN

System Status	Requirement	Fee Required	Action to be taken by the alarm company
New Application for New System	PD6662:2017 & Current BS 8243	1 Fee HUA 1 Fee IAS	Apply to Security Systems Office on Appendix F with Appendix G
New Application for Existing System with no Previous Police Response	PD6662:2004 & DD243:2004 or PD6662:2010 & BS 8243	1 Fee HUA 1 Fee IAS	Apply to Security Systems Office on Appendix F with Appendix 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 BS 8243	N	Apply to Security Systems Office on Appendix F Annexe A
IAS Level 3 (Confirmed systems)	DD243:2002/2004 or BS 8243 90 days clear of confirmed false alarms unless an additional method of confirmation is installed	N	Apply to Security Systems Office on Appendix F Annexe A
Unconfirmed HUA Level 3 (Domestic)	Method of HUA Confirmation either Call-Back, Sequential, Video or Audio.	N	Apply to Security Systems Office on Appendix F Annexe B
Unconfirmed HUA Level 3 (Commercial)	Method of HUA Confirmation either Sequential, Video or Audio.	N	(commercial also) ARC report may be requested to prove Sequential HUA confirmation is in place
HUA Level 3 (Hold-Up Confirmation Failed)	90 days clear of false calls	N	Apply to Security Systems Office on Appendix F Annexe B
HUA Level 3 Confirmation method additional failure	Alternative Method of HUA Confirmation	N	
Deletions			
IAS Deleted Poor Performance	PD6662:2004 & DD243:2004 or PD6662:2010 & BS 8243 + 90 days clear of confirmed false alarms	1 Fee IAS	Apply to Security Systems Office on Appendix F with Appendix G + copy of original installation cert + Annexe A detailing remedial work

HUA Deleted Poor Performance	PD6662:2004 & DD243:2004 or PD6662:2010 & BS 8243 + 90 days clear of false calls + method of HUA confirmation	1 Fee HUA	Apply to Security Systems Office on Appendix F with Appendix G + copy of original installation cert + Annexe B detailing remedial work
Deleted By Alarm Company	PD6662:2004 & DD243:2004 or PD6662:2010 & BS 8243	1 Fee HUA 1 Fee IAS	Apply to Security Systems Office on Appendix F with Appendix G + copy of original installation certificate

APPENDIX G (APRIL 2022)

HAZARDS AND SITE RISKS STATEMENT – HEALTH & SAFETY ACT (MUST BE COMPLETED BY OCCUPIER AT EACH INDIVIDUAL SITE)

Police officers will not normally enter the premises without the keyholder. However, this may be necessary on occasions due to suspicious circumstances. To ensure the safety of officers, the force must be pre-warned of site risks, therefore you are required to state any site hazards in accordance with the Occupiers Liability Act 1957.

Tick (✓) in shaded areas as relevant:

There are <u>NO</u> Hazards							
Hazard Details apply to the Building(s) and Grounds of the Premises						Select (✓) all that apply	
POND		BASEMENT		DOGS		CONTAGIOUS SAMPLES	
SWIMMING POOL		FRAGILE ROOF		DANGEROUS ANIMALS		FLAMMABLE SUBSTANCES	
RIVER FRONTAGE		DANGEROUS STRUCTURE		FIREARMS / SHOTGUNS (excluding air weapons)		FUEL STORAGE	
GLASS COPING WALLS		LOW CEILING BEAMS		AMMUNITIONS		CHEMICALS	
RAZOR WIRE		SLIPPERY FLOORS		EXPLOSIVES		RADIOACTIVE MATERIALS	
INSPECTION PITS		FURNACE		DANGEROUS MACHINERY		ASBESTOS	
SETTLEMENT TANKS		ELECTRICITY SUB STATION		GAS CYLINDERS		SPRINKLER SYSTEM	
VATS		ATM INSIDE PREMISES		TOXIC MATERIALS		FORENSIC MARKER / DYE	
SECURITY FOGGING DEVICE		SMOKE RAID CONTROL (HUA)					
PLEASE NOTE ANY OTHER SITE HAZARDS OR ADDITIONAL FEATURES							

Should site circumstances change you must send an update for our records

1. I am aware that, where applicable, there will be a police alarm administration fee payable (£48.00 + VAT) on the issue of **each** URN or element of a URN
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 authorize that change:

Complete ALL fields:

Customer Signature *		Print Name	
Business name of premises			
Address of protected premises			Tel
Postcode		Date	
Customer email address			

* NB: Typed signatures will not be accepted. Secure electronic or wet signatures are acceptable

Alarm Company - Name			
Alarm Company - Signature		Print Name	
Position in Company		Date	

If this form is not completed correctly your URN Application/Variation form will be returned

APPENDIX H (April 2022)

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 United Kingdom Accreditation Service (UKAS), 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 2 '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 4 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 1 year in advance.
- (h) Terms which transfer inappropriate risks to consumers may be unfair and the Office of Fair Trading (OFT) have suggested that 1 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.policesecuritysystems.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 Consumer Helpline

0808 223 1133

0808 223 1144 (Welsh Language)

www.citizensadvice.org.uk

APPENDIX I (April 2022)

LETTER TO BE HANDED TO POTENTIAL CUSTOMERS BY ALL COMPANIES INSTALLING SECURITY SYSTEMS

Dear Sir/Madam

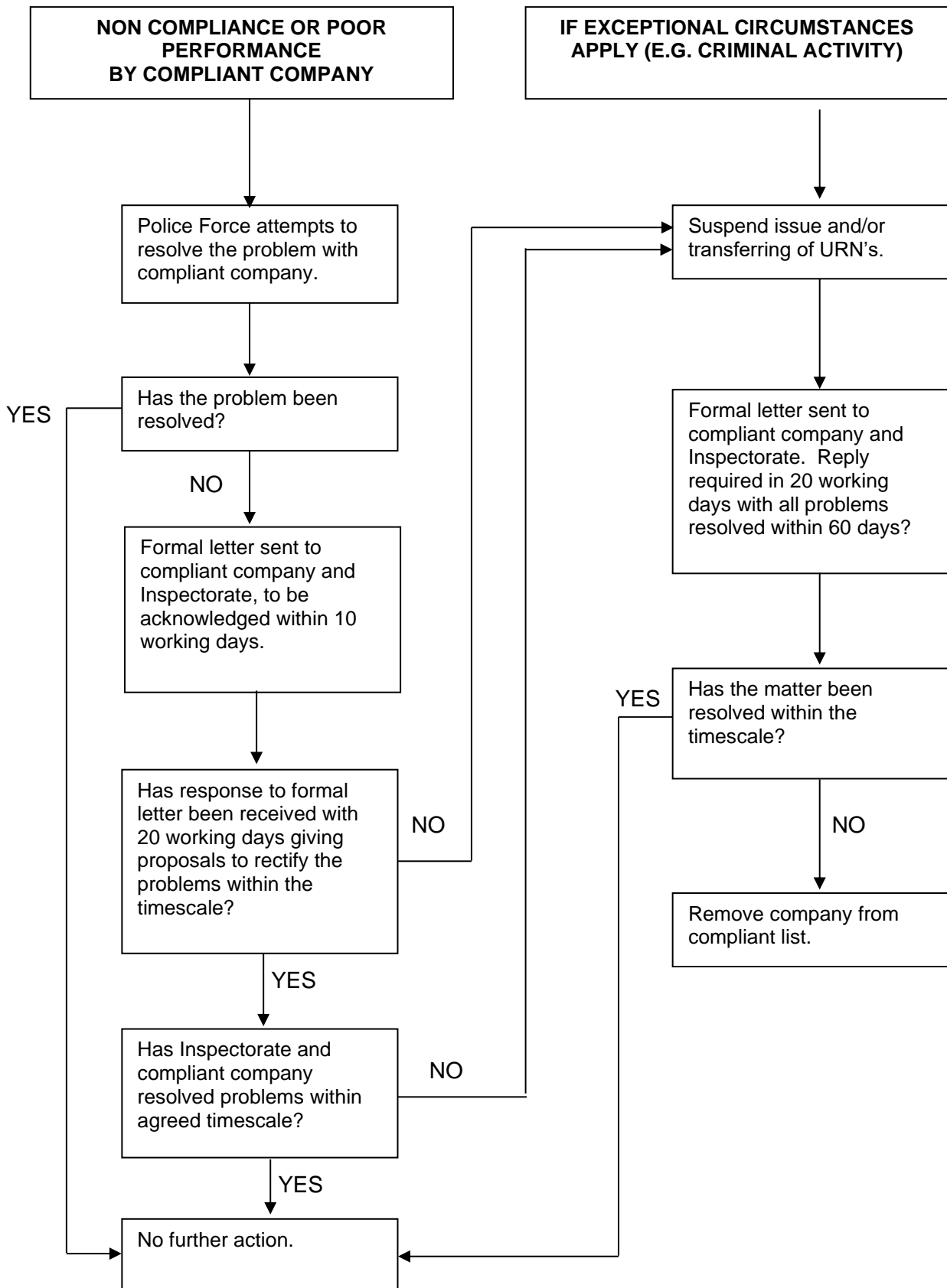
A properly installed security system will help to protect your premises when it is unoccupied. As you are considering the installation of a remote signalling security system you should be aware that the police have safeguards to reduce levels of false calls which divert us away from other tasks in your 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. 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.
5. 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.
6. Following 3 false calls in any rolling 12 month period on your Intruder Alarm police attendance will be withdrawn.
7. If your system has a separate Hold-Up Alarm police response will be withdrawn after 2 false calls in any rolling 12 month period.
8. 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.
9. On completion of the administration procedures your security company will be issued with a Unique Reference Number (URN) which identifies your system within our files to speed call handling. This number should be used in all correspondence to the police but please do not disclose it to any unauthorised person.
10. There is a requirement to have at least two keyholders, details of whom will be maintained by the Alarm Receiving Centre. Keyholders shall be trained to operate the security system, be telephone subscribers, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified.
11. In accordance with the Data Protection Act 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 (April 2022)

MEMORANDUM OF UNDERSTANDING



APPENDIX K (April 2022)

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 2 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 3 (2 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 3 months free of false calls. In the event of restoration of response being delayed for more than 6 months, the URN will be 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 2 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.

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

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 “*HUAs may be operated to summon urgent police assistance when a person is threatened or is in fear of immediate personal violence or criminal act*”. However, in many instances HUAs are used where there is no threat to persons within a defined area. Without knowing the circumstances under which the HUAs are activated, the police must respond. You should be aware that in the current police security requirements, if you use the HUA twice within in a rolling 12 month period and there is no threat to persons in a defined area, you may lose police response.

Accidental misuse happens when staff are not trained in the use of HUAs, 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 or in fear of immediate personal violence or criminal act. 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 (April 2022)

NOTICE OF URN TO INSTALLER

Dear Sir/Madam

RE: (address of installation)

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 (name of force) Police Force Call Handling Centre on (contact number). The message must include the Unique Reference Number (URN) (URN) for use in the Call Handling Centre and failure to quote the URN could result in police attendance being refused.

THE URN 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 PD6662 (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 (April 2022)

LETTER TO BE FORWARDED TO CUSTOMER AT TWO FALSE CALLS

Dear Sir/Madam

Security systems are only 1 example of the demands 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 2 false calls from the system at your premises within a rolling 12 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 3 false calls within a rolling 12 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.

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 (URN).

Yours faithfully

Copy to: (Security System Company)

APPENDIX N (April 2022)

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 **(date)**. 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. 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 Unique Reference Number (URN) element will be deleted from our files.

Yours faithfully

Copy to: **(Security System Company)**

APPENDIX O (April 2022)

LETTER TO SECURITY SYSTEM COMPANY RE REINSTATEMENT OF POLICE RESPONSE

Dear Sir/Madam

RE: Alarm at (address)

Further to your correspondence dated (date), 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

Copy to: (Customer)

APPENDIX P (April 2022)

LETTER TO CUSTOMER ADVISING DELETION OF URN

Dear Sir/Madam

Re: Alarm at (address)

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 Unique Reference Number (URN) allocated to your system with effect from 14 days from the date of this letter.

Your security company has been advised accordingly.

Yours faithfully

APPENDIX Q (April 2022)

LETTER TO SECURITY SYSTEM COMPANY RE DELETION OF URN

Dear Sir/Madam

Re: Alarm at (address)

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 this system with 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 (April 2022)

REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS

1. INTRODUCTION

- 1.1 This document sets out the police requirements for remotely monitored detector activated CCTV systems to enable such systems to gain Unique Reference Numbers (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 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 as called up by BS 8418
- 2.2 RVRCs monitoring detector activated CCTV systems will conform to all of the following standards:
 - BS 5979 (CAT II) or BS EN 50518
 - 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 Information Commissioners Office (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.

5. MANAGEMENT INFORMATION

- 5.1 RVRCs 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.

APPENDIX S (April 2022)

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 BS 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 (SSG) to attend board meetings as an observer for agenda items relating to this scheme.

- I. Be invited to the Security Systems Industry Liaison Group meetings and/or relevant meeting when deemed necessary by the NPCC.
- m. Have and maintain Cyber Essential Plus certification

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 BS 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. 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 – managers may be direct employees or employed on a fixed term contract. 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 **Annexe 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 (to show logging, corrective action and review procedures)

The documented procedures are to the extent necessary to achieve consistency of application.

- g. Operate from suitable premises in the United Kingdom and/or Ireland where confidentiality can be maintained and with adequate safeguards for security of information on a 24 hour basis.

Note: Any company seeking to operate outside of the United Kingdom or Ireland can only do so with the express permission of the NPCC SSG whose decision will be final.

Guidance – Any security system used for the purpose of protecting the alarm company premises shall comply with the minimum standards of these procedures. Alarm receiving centres and/or monitoring centres must comply with the appropriate standards in **Annexe A**.

- h. Have the necessary resources to support 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. 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 **Annexe A**.
- k. Have customer contracts describing the products and services to be supplied together with the associated terms and conditions.
- l. 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.
- i. All electronic and telephone communication, by whatever means, with potential and existing customers shall be in accordance with the Privacy & Communications (EC Directive) Regulation 2003 (PECR), see the Information Commissioners Office Direct Marketing Guidance document at <https://ico.org.uk/media/1555/direct-marketing-guidance.pdf>
 - ii. all face-to-face doorstep sales staff (directly or indirectly employed) shall comply with the Consumer Contracts (Information and Additional Charges) Regulation 2013. All door-to-door sales shall be compliant with the law, further guidance can be found at <https://www.gov.uk/doorstep-selling-regulations>
- n. Ensure monitoring and maintenance contracts for **domestic premises** shall not exceed a period of 3 years and payments in advance shall not exceed 1 year.

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

V Where amendments to this scheme are deemed appropriate by the NPCC, a consultation meeting will be instigated for attendance by those concerned.

APPENDIX S – ANNEXE A (April 2022)

BRITISH STANDARDS AND EUROPEAN NORMS

(Current issue unless stated – see notes)

BS 4737	Intruder Alarms in Buildings (mostly withdrawn see notes)
BS 7042	High Security (withdrawn see notes)
BS 8418	Remotely monitored detector activated CCTV Systems
BS 5979	Alarm Receiving Centres (Category II) (withdrawn see notes)
BS 8591	Alarm Receiving Centres (not Intruder & Hold up Alarms)
BS 6799	Wire free Alarms (withdrawn see notes)
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 (withdrawn see notes)
PD 6662:2004	Scheme for the application of European Standards for intruder and Hold-Up Alarm systems (withdrawn see notes)
IA 1501:2015	Industry agreement on PD 6662:2010
PD 6669:2017	Guidance for the Provision of Alarm Transmission Systems (ATS) (optional standard – to be reviewed April 2020)
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 PD 6662)
BS 8473	Management of False Alarms
BS 8243	Installation & configuration of Intruder & HUAs designed to generate confirmed alarm systems (applies under PD 6662)
BS 8484	Provision of Lone Worker Device Services
BS 8593	Code of Practice for the deployment and use of body worn video

BS 9518 Code of Practice for processing of alarm signals by an Alarm Receiving Centre (when published)

British Standards Institution Drafts for Development (Latest Issue)

BS DD 242 High Security (withdrawn see notes)

BS DD 243 Applies under PD 6662:2004 (withdrawn see notes)

BS DD 244 Wire Free Alarms (withdrawn see notes)

BS DD 263 Alarms Systems Commissioning, Maintenance and remote support (applies Under PD 6662)

BS 9263:2016 Alarms Systems Commissioning, Maintenance and remote support (applies Under PD 6662:2017)

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 notes)

DD CLC/TS 50131-7:2003 Applies under PD 6662:2004 (withdrawn see notes)

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.

Some older and withdrawn standards or parts of standards are still included in this list for the benefit of legacy systems that remain in service

Cyber Security Guidance

NPCC recognises the need to include cyber security as a holistic part of a security system and includes the following as best practice guidance to installers:

1. *Installation of Safety and Security Systems – Cybersecurity Code of Practice* (form 342 published by BSIA)
2. Cyber Essentials / Cyber Essential Plus
3. Payment Card Industry Data Security Standard (PCIDSS)

Notes:

At this time the above guidance is not mandatory for companies claiming compliance with NPCC requirements

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 (April 2022)

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.

See **Appendix F Annexe C** re restoration of HUA.

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

Restricting duress codes to high security systems ensures 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:

- I. In premises that require high security and duress has been identified as an essential requirement from the risk assessment
- II. Duress is notified separately from the hold-up alarm signal
- III. 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 HUAs, e.g. care alarm type systems being used for HUAs. 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

Not in use

APPENDIX V (April 2022)

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 Lone Worker Devices (LWD) 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, how to cancel any false activations that occur so as to minimise any false calls and be provided with a copy of **Appendix V Annexe A**.

2. URN REQUIREMENTS

- 2.1 The monitoring centre will apply to the relevant police force for a URN using **Appendix F** of these requirements. The cost of the URN will depend on the number of devices monitored nationally:
 - Under 10,000 £58.00 plus VAT per annum.
 - 10,000 – 50,000 £87.00 plus VAT per annum.
 - 50,000 or above £116.00 plus VAT per annum.
- 2.2 Lone worker URNs are renewable annually on the 1st April. The monitoring centre is to advise the police alarm administrator of renewal 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 LWDs shall meet the lone worker device requirements laid down in BS 8484.
- 4.2 Body Worn Video (BWV) 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. 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 EN 50518 and BS 9518 if required

- 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

- 6.1 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 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 only be reinstated once the supplier has proven 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 Group (SSG) 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 incident.
- 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 location, 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.
- 8.6 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 2018.

9. MANAGEMENT INFORMATION

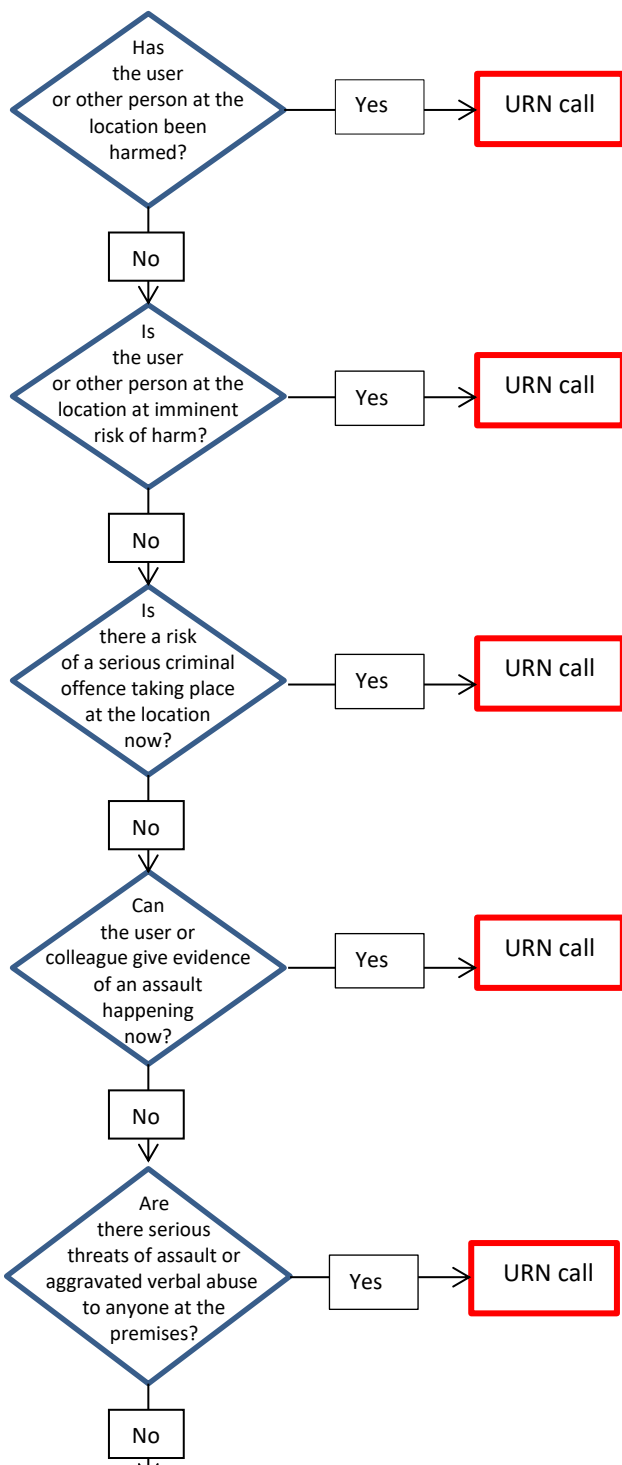
- 9.1 The monitoring centre and the supplier shall ensure that they have a false alarm management system in place.
- 9.2 The monitoring centre shall hold statistics on all their customers and when required provide the police with relevant data.
- 9.3 The monitoring centre shall inform the customer when false alarms occur and when the customer is about to lose police response.

10. INDEMNITY

- 10.1 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 lone worker if the location information is not accurate.

APPENDIX V – ANNEXE A (April 2022)

USE OF 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 lone worker 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 LWD 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 behavior 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 at a fixed site *does not* include non-emergency situations, including:

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

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

Call police using 101 or 999 (see panel below for further information)

Note: Part 2 – Use of Lone Worker Device advice to ARC operators

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 at the premises

External situations – use 999 for:

- Public order outside of the premises
- Criminal offence in progress outside of the premises

Contacting the police when using the URN system – the ARC should say:

- “This is a Lone Worker Personal Attack Alarm URN XXXX”

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 and/or 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.