

Police Service of Scotland Security Systems Policy

DRAFT FOR CONSULTATION

Version 0.12
Jan 2012

Contents

Document Information	4
Version Control	5
Version Distribution	8
DEFINITIONS	9
1. INTRODUCTION	12
1.1 Scope of Policy	12
2. AIMS OF THE POLICY	12
3. GUIDANCE ADVICE AND PROCEDURES.....	12
3.1 Type A systems.....	12
3.2 Type B systems.....	14
3.3 Accredited Monitoring Centres	15
3.4 Non-Accredited Monitoring Centres	15
3.5 List of Compliant Companies Installing Type A Security Systems	15
3.6 Information to Customer.....	16
3.7 Notice to Customer Type A Systems	16
3.8 Notice to Install a Type A Security System	16
3.9 Variations of URN Application Details	17
3.10 Keyholder Details for Monitored Systems.	17
3.11 Delays of Audible Sounder and Alarm Activated Security Devices	18
3.12 False Alarm Monitoring	18
3.13 Administrative Charges	19
3.14 Memorandum of Understanding	20
4. POLICE RESPONSE	20
4.1 Police Attendance - Type A Security Systems	20
4.2 Remote Detector Activated CCTV Systems	24
4.3 Remote Detector Activated CCTV Systems	24
4.4 Vehicle Tracking Systems.....	24
4.5 Police Attendance - Type B Security Systems	24
5. LEGISLATIVE REQUIREMENTS.....	25
5.1 Data Protection Act 1998	25
5.2 European Court of Human Rights	25
5.3 Freedom of Information (Scotland) Act 2002	26
5.4 Racial Equality	26
5.5 Advertising	26
6 UKAS CERTIFICATION BODIES AND RESPONSIBILITIES.....	26
6.1 Certification Bodies and Requirements	26
7. POLICE REQUIREMENTS (Final Discretion).....	27

7.1	Right of Refusal.....	27
7.2	Policy Amendment Requests	27
7.3	Copyright.....	27
	INDEX TO APPENDICES.....	28
	Appendix A - Policy variations to Force service standard	29
	Appendix B - Application to be accepted on Police list of compliant companies/policy agreement form	30
	Appendix C - Disclosure of Convictions.....	32
	Appendix D - False alarm monitoring formula.....	35
	Appendix E - Administration Charges	37
	Appendix F Annexe A - Application for restoration of Police response to an intruder alarm	41
	Appendix F Annexe B - Application for restoration of Police response to a hold up alarm	43
	Appendix G - Hazards and site risk statement (Health & Safety)	46
	Appendix H - Police advice to members of the public seeking information on security companies	49
	Appendix I - Letter to be handed to potential customers by all companies installing security systems.....	51
	Appendix J - Memorandum of understanding	53
	Appendix K - Police letter to customer on completion of installation.....	54
	Appendix L - Notice of URN to installer	56
	Appendix M - Letter from the Police to customer at three false calls	57
	Appendix N - Letter from Police to customer advising withdrawal of response.....	58
	Appendix O - Letter from Police to customer reinstating Police response	58
	Appendix P - Letter from Police to customer on deletion of unique reference number	59
	Appendix Q - Letter from Police to security system company on deletion of unique reference number	61
	Appendix R - Requirements for companies installing and monitoring remote CCTV systems	62
	Appendix S - Requirements for security system services	65
	Appendix S Annexe A - British Standards and European Norms	69
	Appendix T - Ten point plan for hold-up (personal attack) alarms	71
	Appendix U - Requirements for companies installing and monitoring after-theft systems with vehicle immobilisation for vehicle recovery	74
	Appendix U annexe A - Police Service of Scotland vehicle tracking requirements	78
	Appendix U Annexe B - After-theft vehicle immobilisation systems indemnity.....	79
	Appendix V - Police requirements for lone workers services	81

Document Information

Document Title	Police Service of Scotland Security Systems Policy
Version	DRAFT 0.12
Police Service of Scotland Business Area	Working with the public
Publication date	20/01/2013
Author(s)	Police Service of Scotland security systems subgroup
GPMS Marking	Not Protectively Marked
Reason for GPMS higher than Not Protectively Marked	N/A
Disclosable under the Freedom of Information (Scotland) Act 2002?	YES
Publishable under Scottish Police Publication Scheme?	YES
If NO, provide reason	N/A
Document Review	
Equality Impact Assessment	YES
Full EIA or Screening Document?	Full EIA
Date of assessment	17/07/2012
Police Service of Scotland Publication No.	

The effectiveness and ongoing relevance of this document will be subject to review by the Police Service of Scotland business area(s) detailed above.

The next review of this document is due by [insert date]; however, it will be updated according to significant legislative and policy changes and re-released earlier, if required.

Version Control

Version	Date	Authorisation	Information
0.1	10/02/2012	PF	New version of Security Systems policy to replace existing version. Multiple changes in policy.
0.2	24/02/2012	PF	Corrections to 2.1 / 3.1a/ 3.1b/ 3.3.4 / 3.3.4b/ 3.4.1/ 3.7.7/ 3.9.4/ 3.11.2/ 3.12.1/ 3.12.4/ 3.12.5/ 3.12.6/ 3.12.7/ 4.1.5a/ 4.1.5b/ 4.1.6/ 4.1.7/ 4.2.5/ 4.5/ 4.51 following sub group review.
0.3	05/03/2012	PF	Further corrections to 5.11/ 5.3.2/ 7.1/ 7.2/ Appendices A/ C/ D/ F/ G/ I/ R/ T/ U and alignment of columns.
0.4	08/03/2012	PF	New sections 3.2 & 3.3, subsequent renumbering. Update of all dates for change to take place starting September 2012 instead of March. Change of terminology to Chief Constable. New sections 4.6.3 and 4.6.4. Drop down issues in Appendix F work outside of Police system if the document is protected.
0.5	27/03/2012	MR	Option of alternates within appendix C, plus addition of overseas checks in appendix C & draft marking
0.6	11/05/2012	PF	Change date from June to September in 3.13.1

			and 3.13.7
0.7		MR	Changes following legal review of document. Definitions table added, minor changes to paragraph ordering and content.
0.8	29/09/2012	PF	Minor changes as a result of force reviews and change of implementation dates (Shows Version 7 + 8 changes in track changes).
0.9	29/10/2012	PF	Change of implementation date to April 2013 introduction of installation certificates as a requirement before issue of URN. Annual renewal clause for ATSVIVR SOC's removed. Change to 3.5.1 ref Accredited company obtaining URN's for non-accredited companies.
0.10	01/11/2012	PF	Change from Police Service of Scotland to Police Service of Scotland
0.11	07/11/2012	PF	Removal of ACPOS and replacement with Police Service of Scotland/ transfer of detail from appendix A into policy standards/ Font size change to Arial 12/ some date corrections in appendices
0.11b	22/11/2012	PF/MR	Slight changes in naming convention – still incorporating version 11 changes

0.12	20/01/2013	PF/MR	Minor modifications.
------	------------	-------	----------------------

[Version numbering convention – Minor changes to the document should be numbered v1.1, v1.2 etc. when a new version with minor changes is approved and published; Where there are significant changes; for example, new chapters, change of policy etc., the new version should be numbered v2.0, v3.0 etc, once the new document is approved and published]

[Tracking of draft versions is the responsibility of the business area and details should not be included in the published document]

DRAFT FOR CONSULTATION

Version Distribution

Version	Date	Information
0.1	10/02/2012	ACPOS Security Systems sub group for review
0.2	24/02/2012	ACPOS Security Systems sub group for review
0.3	05/03/2012	ACPOS Security Systems sub group for review
0.4	08/03/2012	ACPOS Security Systems sub group for review
0.5	27/03/2012	ACPOS Security Systems sub group for review
0.6	11/05/2012	ACPOS Security Systems sub group for review
0.7		
0.8	29/09/2012	ACPOS Security Systems sub group for review
0.9	29/10/2012	ACPOS Security Systems sub group for review
0.10	01/11/2012	ACPOS Security Systems sub group for review
0.11	07/11/2012	ACPOS Security Systems sub group for review
0.11b	22/11/2012	ACPOS Security Systems sub group for review
0.12	20/01/2013	ACPOS Security Systems sub group for review

DEFINITIONS

Alarm Receiving Centre (ARC) / Remote Video Response Centre (RVRC) / System Operation Centre (SOC)	Control Centres forming part of the commercial security industry that monitor security systems, alarm activations etc.
Bacs	Bacs is a not-for-profit, membership-based industry body owned by 16 of the leading banks and building societies in the UK, Europe and US. It is responsible for the schemes behind the clearing and settlement of automated payments in the UK including Direct Debit and Bacs Direct Credit.
British Security Industry Association (BSIA)	The British Security Industry Association is the trade association for the professional security industry in the UK.
CCTV	A system which sends television signals to a limited number of screens, and is often used to prevent crime.
Chief Constable	The post of Chief Constable leads a senior management team within the Police Service of Scotland and has overall responsibility for the administration and management of Police operations. The Chief Constable's obligations relating to this Policy are discharged by the Police Alarms Administration Department.
Criminal Records Bureau (CRB), Access Northern Ireland	Disclosure Scotland equivalent bodies in England & Wales, and Northern Ireland.
Command and Control Custodian	The Command and Control Custodian is responsible for the administration of the National Command and Control system which includes Security Systems

	administered through the National Command and Control System.
Compliant Companies	Security companies inspected by UKAS accredited inspection bodies, which have agreed to comply with the requirements of this Policy.
Confirmation Technology	A method of confirming alarm activations are genuine through a system of electronic, audio, or visual, alarm verification.
Confirmed/Unconfirmed Systems	Security systems that incorporate/do not incorporate Confirmation Technology.
Data Processing Unit (DPU)	This unit was set up with the intention of the eventual centralisation of Command and Control administrative services in the Police Service of Scotland including alarms administration.
Disclosure Scotland	Disclosure Scotland is designed to enhance public safety by providing potential employers and voluntary sector organisations with criminal history information on individuals applying for posts.
Disclosure Scotland Basic/Enhanced Disclosure Certificate	Criminal history information provided by Disclosure Scotland outlining criminal convictions (basic certificate), and may also contain information held by Police forces and other Government bodies (enhanced certificate)
False Alarm Activations/False Calls	Security system activations resulting from a reason other than criminal attack/incident.
Freedom of Information Officer	A representative of the Police Service of Scotland who has responsibility for discharging relevant statutory obligations under the

	Freedom of Information (Scotland) Act 2002.
Key Holder	A person who will provide access to premises etc and operate alarm equipment in the event of an alarm activation.
Police Alarms Administration Department	The Police Service of Scotland administration department responsible for managing security system records and administering URNs.
Security Industry Authority (SIA)	The Security Industry Authority is the organisation responsible for regulating the private security industry in the United Kingdom.
Security System	An electronic system that detects alarm conditions and generates alarm signals.
Unique Reference Number (URN)	Police reference number which identifies security system within Police systems to speed call handling.

1. INTRODUCTION

1.1 Scope of Policy

- 1.1.1** The Police Service of Scotland Security Systems Policy replaces the existing ACPOS security Systems Policy 2010. This new policy recognises the rapid development of technology and its use within security systems. This policy details the Police response which can be expected to an electronic security system (e.g. Intruder and Hold-up alarm system, Lone worker device, detector activated CCTV vehicle tracking system).
- 1.1.2** In view of the excessive number of false activations emanating from security systems, the Scottish Police service has found it necessary to adopt a policy relating to the design, installation, commissioning maintenance, repair and proper use of such security systems.
- 1.1.3** The policy is fully authorised and endorsed by Police Service of Scotland in consultation with the security industry and other relevant parties. Any variation in the policy must be authorised by the Police Service of Scotland.

2. AIMS OF THE POLICY

The aims of this policy are:

- a. To improve the quality management of security systems
- b. To reduce the volume of false activations notified to the Police
- c. To allow the Scottish Police service to maximise their use of resources

3. GUIDANCE ADVICE AND PROCEDURES

This Police Service of Scotland policy deals with two types of security systems:

Type A (accredited systems) and Type B (non accredited).

3.1 Type A systems

Security systems that meet the requirements of this policy and are remotely monitored will be deemed Type A systems and will be prioritised for an immediate Police response subject to available resources at time of incident as set down in Section 4.1.

Type A - Remote Signalling Systems.

- 3.1.1** Security system signals will terminate at an ARC, or RVRC for CCTV or SOC for vehicle tracking conforming to British Standard (BS) 5979 (Cat II) and the requirements of this Police Service of Scotland policy.
- 3.1.2** All security systems stated in this Police Service of Scotland policy shall meet the requirements of the relevant standard listed in **Appendix S** of this Police Service of Scotland Policy. *Note: New Hold-up alarms are not required to be installed using confirmation technology, but Hold-up confirmation technology will be required to bring the system back on response after losing Police response.*
- 3.1.3** Automatic 999 dialling alarm equipment is not permitted.
- 3.1.4** All central monitoring station alarm messages must be transmitted to our Force Control Room on dedicated ex-directory telephone lines. The number of which will be disclosed on receipt of a signed policy agreement (Appendix B).
- 3.1.6** All correspondence should be addressed to the Supervisor, Police Service of Scotland Alarms Administration Department.
- 3.1.7** The Unique Reference Number (URN) remains the property of the Police Service of Scotland 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
- 3.1.8** Unique reference numbers (URNs) will only be issued to security systems compliant with this policy. In the case of stolen vehicle tracking systems and lone worker systems, the URN will be issued by the Police Service of Scotland Alarms Administration Department to the SOC or ARC direct. (Note: URNs are owned by the Police Service of Scotland Alarms Administration Department and are used for administration purposes only; they do not guarantee a Police response).
- 3.1.9** Prior to 1st April 2013 intruder and hold-up alarm systems (I&HAS) have been allocated one URN for a combination intruder and hold-up alarm. From 1st April 2013 this will change to, where part of the system goes off response (see sections 4.1.5 and 4.1.6) then for single URN systems :
- a) If the intruder part moves to level 3 then clauses 4.1.10 of the policy applies and the hold-up part of the alarm will be set up as a separate hold-up alarm urn free of charge and will continue to receive response if the customer still requires their hold up alarm. (Note: after 1st April 2013

if a new intruder system including a hold up alarm is installed then the hold up alarm will require its own URN. See clause 3.13.7).

- b) If the hold-up alarm part triggers a level 3 response due to false activations then clause 4.1.15 and 4.1.16 applies. A new intruder URN will need to be set up which will be free of charge for existing systems if the customer still requires their intruder alarm. (Note: after 1st April 2013 if a new intruder system including a hold-up alarm is installed the, hold-up alarm will require its own URN. See clause 3.13.7

3.1.10 Confirmation technology (BS 8243 applies) is mandatory for newly installed intruder alarms (confirmation does not apply to new Hold up alarm systems) and for all I&HAS that lose Police response (drop to level 3) and wish to regain a Police response (back to level 1). Police response to line cuts for monitored security systems that have lost Police response will be at the discretion of the Force.

3.1.11 ARCs dealing solely with security systems within their own company premises (in-house monitoring), are exempt from the BS5979 Cat II certification provided:

the facility was operational with Police consent prior to 31st October, 1995,

AND

there has been no change of premises;

AND

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

The security systems are operated in accordance with all other aspects of this policy.

3.2 Type B systems

Security systems that do not meet the requirements of this policy (e.g. bells only systems) will be deemed to be Type B systems and will not be given a Police response unless the requirements of clause 4.5 are met. Also security systems installed by companies who are not members of UKAS accredited Inspectorates will be regarded as non-standard and will be dealt with as a type B system.

(Note: A security systems can be any type of electronic security alarm system (e.g. Intruder alarm, Hold-up alarm, lone worker alarm, vehicle tracking alarm, detector activated remote monitored CCTV).

3.3 Accredited Monitoring Centres

The installation and services provided by the Compliant Companies, such as security companies, lone worker supplier and ARC's shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of this Police Service of Scotland Policy. (Note: See **Appendix S**)

3.4 Non-Accredited Monitoring Centres

Non – accredited Alarm Receiving Centres will not receive a Police response in accordance with section 4.5.2 of this policy.

3.5 List of Compliant Companies Installing Type A Security Systems

3.5.1 Only companies belonging to UKAS accredited inspectorates (see **Appendix H**) with the scope for security systems and this policy will be deemed to be compliant and have the ability to gain a URN for their customers.

UKAS accredited companies found to be obtaining URN's on behalf of non –accredited companies will be removed from the accredited companies list.

Inclusion on a UKAS accredited Inspectorate list does not amount to confirmation that the company or its work has been inspected by the Police.

3.5.2 Only companies so listed may install, maintain and/or monitor Type A systems in the particular Police area.

3.5.3 Where a company loses Police recognition under this policy, its existing customers will have 3 months in which to make alternative maintenance/monitoring arrangements or their URN's will be removed from the system and any alarm activations will be dealt with as a type B system.

3.5.4 Where a customer changes to an accredited company within the three month period the URN will be provided free of charge.

3.5.5 Compliant companies will meet the requirements laid down in **Appendix S** of this policy.

3.5.6 The company shall not have as a principal or employ in the surveying, sale, installation, maintenance or administration of security systems persons with criminal convictions (other than spent convictions). Appendix C sets out a procedure for the implementation of this requirement.

3.5.7 The company shall take responsibility for ensuring that it updates itself with amendments to this Police Service of Scotland Policy.

3.6 Information to Customer

- 3.6.1** 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**.

3.7 Notice to Customer Type A Systems

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

3.8 Notice to Install a Type A Security System

- 3.8.1** Notice of intention to install a Type A security system requiring a URN, shall be sent to the Chief Constable in the form of **Appendix F** and **Appendix G** and inclusion of a copy of the **NSI/SSAIB certificate of installation for the property**.
- 3.8.2** All notices or other documents required for the issue or processing of a URN may be sent by electronic means or post as defined by the Police Service of Scotland Alarms Administration Department.
- 3.8.3** This will result in the issue of a URN, which must be quoted in any communication regarding the installation. An alarm activation received from an ARC/RVRC without a current Police URN will be treated as a Type B system and not receive a Police response without additional evidence of an offence in progress.
- 3.8.4** If an electronic application process facility exists between the Police and the alarm installation company, a notification of URN number will be sent through a secure electronic method allocating a URN against the transaction number.
- 3.8.5** Electronic application facility can be withdrawn from a company or companies at Police discretion.
- 3.8.6** All written applications must enclose a stamped addressed envelope for return notification of the URN.
- 3.8.7** The Unique Reference Number remains the property of the Police Service of Scotland Alarms Administration Department and must be quoted in all correspondence. In the interests of maintaining security of records, all enquiries concerning individual alarm systems must be made in writing or

through the Police approved secure electronic system. **Telephone enquiries regarding specific systems or particular alarm activations will not be accepted and all such enquiries must be made in writing.** Only Police Service of Scotland Alarms Administration Department can withdraw or transfer URN

3.8.8 Facilities for inspection of the alarm installation shall be made available if required by the customer to the Chief Constable.

3.9 Variations of URN Application Details

3.9.1 The Chief Constable shall be notified within 28 days of any variation to the original URN application details, in the form of **Appendix F**. Failure to notify of any variations may lead to subsequent cancellation of the URN requiring a new application to be submitted.

3.10 Keyholder Details for Monitored Systems.

3.10.1 All premises with Type A security systems shall have at least two key holders, details of whom will be maintained by the ARC/RVRC, It is the responsibility of the system user to notify the installer/ARC of any keyholder changes. Failure to comply with these instructions could result in the URN being suspended.

3.10.2 Keyholders will;

- a) be trained to operate the alarm
- b) be contactable by telephone
- c) have adequate means of transport to attend the premises at all hours
- d) have access to all relevant parts of the premises
- e) be able to attend within 20 minutes of being notified
- f) be contacted by the ARC/RVRC in the case of any activation of the security system.

3.10.3 The maintenance of monitored alarm key holders records is the responsibility of the ARC/RVRC, not the Police. ARC/RVRC will re-contact key holders or key holding company when requested to do so by the Police control room following an activation if the key holder has not attended the premises within the 20 minute period (from the time of incident creation at the Police control room).

3.10.4 ARC / RVRC will supply details of keyholders as required by Police for relevant policing purposes.

3.10.5 Customers who employ a commercial key holding company must be aware of the Security Industry Authority (SIA) Licensing Regulations in relation to key holding and response. More information can be obtained from www.sia.homeoffice.gov.uk

3.10.6 Failure of key holders to attend when requested within the 20 minute travel period on three occasions in a rolling twelve month period will result in the withdrawal of Type A Police response for a three month period. Exceptions to this will be at the discretion of the force. During this period, response will only be on the basis that there is additional evidence that a crime is being committed. Property owners will be advised of this restriction by letter or e-mail and will be responsible for advising their insurance company of the reduced level of response.

3.11 Delays of Audible Sounder and Alarm Activated Security Devices

3.11.1 There is no requirement for security systems to have audible or visual warning devices delayed following activation of the system. However, premises may be required to have their warning devices delayed for a maximum of 10 minutes where the Chief Constable determines that the call handling time, location or type of premises and the Force Service Standard would enable officers to attend the premises within that time. This will be intimated directly to the security system installer.

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

3.12 False Alarm Monitoring

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

3.12.2 Definition – For the purpose of this policy, a false alarm is an alarm call which has been 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/lone worker/RMDA CCTV system (see Appendix R) made with good intent.

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

- 3.12.3** It is the customer's obligation to ensure that Police have accurate information in relation to any alarm activations.

3.13 Administrative Charges

- 3.13.1** Each application for a URN is subject to an administration fee payable by the system user. The URN fee is £43.49 plus VAT from 1st April 2013. Acceptable methods of payment (which may include BACS) and will be reviewed by the Police Service of Scotland annually. The current policy on charging is set out in **Appendix E**. URNs for vehicle tracking and lone worker services are dealt with in **Appendix U & Appendix V** of this policy.
- 3.13.2** Where an electronic facility for application has been approved between the force and Security systems companies, the Police Service of Scotland may provide secure electronic payment methods which may include an invoicing facility. Police Service of Scotland Alarms Administration Department reserve the right to withdraw this facility from a company or companies temporarily or permanently
- 3.13.3** Police Service of Scotland Alarms Administration Department may provide an online secure facility by arrangement with security system installers which will hold basic status details of their security systems held by the URN number only. The Alarms Administration Department reserves the right to withdraw this facility from a company or companies temporarily or permanently,
- 3.13.4** The Administration fee charged by the Police 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 installation company.
- 3.13.5** For I&HAS and CCTV systems the installation/maintenance company will if requested, pay an invoice from the Police for the payment of the URN administration 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 version of this policy.

3.13.6 If the company pay an invoice referred to in 3.13.5 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.

3.13.7 Any systems applying for URN's after 1st April 2013 will need to apply separately for intruder and hold-up alarm URN's and any joint I&HAS that is in a withdrawn state that applies for re-instatement will need to apply for separate intruder and hold-up alarm URN's.

3.13.8 *Any joint I&HAS that exist on the system that are in a withdrawn state and are applying for re-instatement, will need to apply using the correct URN relevant to the Intruder or Hold-up part of the system which exist at the location.*

3.14 Memorandum of Understanding

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

4. POLICE RESPONSE

4.1 Police Attendance - Type A Security Systems

4.1.1 For Type A security systems there are three levels of Police alarm status.

a) Level 1 – Immediate/Urgent

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

b) Level 2 – Warning state - Police attendance desirable but will be dependent on resource.

c) Level 3 – Withdrawn

No Police attendance, key holder response only unless there is other evidence of criminality (i.e. type B response).

4.1.2 Police Service of Scotland has adopted a policy on the use of confirmed alarm technology as part of the effort to reduce false calls.

4.1.3 All new applications will only qualify for a URN and Police response if installed to the current required standard (e.g. the current PD6662 scheme

for application of European Standards for I&HAS). (*Note: New Hold-up alarms are not required to be installed using confirmation technology, but Hold-up confirmation technology will be required to bring the system back on response after losing Police response*).

4.1.4 Police Service of Scotland has designated that all I&HAS installed to DD 243:2002 onward are designated as a “confirmed” system and any I&HAS installed prior to DD 243: 2002 is designated as an “unconfirmed” system.

4.1.5 The number of false alarms allowed for security systems **subject to the provisions of section 3.12.2** (excluding lone worker and vehicle tracking systems – See 4.1.7) will be:

- a) From 1st April 2013, security systems issued or with an existing URN will receive level 1 response until **three** false calls have been accrued within a rolling 12 month period, then the security system will drop to level 2. If **two** more false calls are accrued within the 12 month rolling period then the security system will drop to level 3.
- b) From 1st April 2014 security systems will only be allowed **two** false calls before the security system drops to level 2 and then if the security system has **one** further false alarm within the rolling 12 month period the system will drop to level 3 and lose Police response.
- c) **In all cases (other than those highlighted in section 3.12.2) the system will drop to level 3 if the maximum number of false calls has been reached within a 12 month rolling period, irrespective of whether a warning notice has been issued by the Police.**

4.1.6 Once the number of false alarms triggers a level 2 response, the Police Service of Scotland Alarms Administration Department will send a warning letter to the customer informing the customer of this. If the total amount of false alarms reach the level for the security system to move to level 3, the Alarms Administration Department will send a letter to the customer informing them that Police response will be withdrawn and a copy will also be sent to the maintaining company. At level 3 the security system will be treated as a type B security system and will not receive a Police response, unless further evidence of criminality is provided for an incident. The customer will be advised in writing that their security system is on LEVEL 3 and a copy will be sent to the maintaining company. The maintenance company on receipt of a withdrawn response letter shall instruct the ARC/RVRC not to pass any further alarm messages to the Police.

TABLE 1

Time Period	Total False alarm activations within a rolling 12 month period	resultant alarms status level	communication to customer and installer
1st April 2013 - 31st March 2014	Less than 3	1	none
	3	2	Warning Notification sent to installer and customer
	5 or more	3	Withdrawn - installer and customer notified
1 st April 2014 onwards	Less than 2	1	none
	2	2	Warning Notification sent to installer and customer
	3 or more	3	Withdrawn - installer and customer notified

4.1.7 For lone worker systems and vehicle tracking systems, the false activations trigger before a warning and subsequent removal of response by Police will be detailed within **Appendix U & Appendix V**

4.1.8 Where an ARC has been advised by the installer that a security system is in a withdrawn or in a deleted state, they will ensure that no activations are passed through to the Police. A level 3 response will apply in such circumstances.

4.1.9 Only when the Police are satisfied that the security system is operating efficiently will Police response upgrade to level 1 be considered.

4.1.10 For I&HAS following withdrawal of Police response (i.e. level 3), the following conditions will apply in order to reinstate Police response:

- a) Unconfirmed I&HAS will need to be upgraded with confirmation technology to a confirmed BS8243 system (all I&HAS installed prior to DD243 2002 are designated unconfirmed).
Reinstatement of Police response may be achieved, without a 3 month delay, following compliance with the above. Where a system has been upgraded, a copy of the NSI Compliance/ SSAIB Conformity certificate will be required by the Police.

- b) Confirmed I&HAS with DD243 (2002 / 2004) or BS8243 I&HAS will require the cause of the false alarms identified, remedial action taken and a period 3 months free of false calls (supported by evidence from the security company).

The Security Company should apply for reinstatement of response using **Appendix F – Annexe A**.

- 4.1.11** Should the level of false calls result in the restoration of response being delayed for more than 6 months, the URN for the relevant intruder or hold up parts of the system will be deleted and the occupier and the security company advised in writing
- 4.1.12** After deletion of a URN any subsequent application for re-instatement will be deemed to be a new application and must meet the full requirements of **Appendix S**
- 4.1.13** In an I&HAS, the remote signals sent to the ARC shall differentiate between hold-up (personal attack) and the intruder alarm signals.
- 4.1.14** A **Hold-up alarm** may be operated as part of a security system to summon urgent Police assistance when persons within premises are under immediate attack or threatened attack.
- 4.1.15** The Hold-up alarm system, which conforms to the agreed standards set down in **Appendix S**, will attract a level 1 response. When misuse of the system is identified as per 4.1.5 in a twelve-month period, response may be downgraded to level 3. This will be considered after the force has undertaken a Police assessment on the premises in question.
- 4.1.16** Following withdrawal, reinstatement will be considered following a further Police assessment or the URN will be deleted after 6 months in a withdrawn state.
- 4.1.17** Hold-up alarm systems conforming to section 4.1 will attract a level 1 response. Where the threshold for withdrawal of Police response is reached the withdrawal will apply to the facility (intruder or hold-up) 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 and Police response is then withdrawn. Reinstatement of intruder alarms is dealt with in clause 4.1.10 and hold-up alarms is dealt with in clause 4.1.16.
- 4.1.18** Joint intruder /hold-up systems prior to 1st April 2013 or systems which have been allocated one URN for a combination intruder and hold-up alarm – where part of the system goes off response then:

- a) if the intruder part moves to level 3 then clauses 4.1.10 of the policy applies and the hold-up part of the alarm will be set up as a separate hold-up alarm urn free of charge and will continue to receive response.
- b) If the hold-up alarm part triggers a level 3 response due to false activations then clause 4.1.15 & 4.16 applies. A new hold-up URN will need to be requested which will be free of charge for existing systems if the customer still requires their hold-up alarm.

4.2 Remote Detector Activated CCTV Systems

- 4.2.1 To enable **remote detector activated CCTV systems** to gain a URN for Police response, systems are to be installed and maintained to the standards and requirements specified in **Appendix R**

4.3 Remote Detector Activated CCTV Systems

- 4.3.1 For **lone worker devices** where the ARC is accredited in accordance with BS5979 (Cat II) and the systems in accordance with BS8484, a single URN will be allocated to the ARC in accordance with **Appendix V**

4.4 Vehicle Tracking Systems

- 4.4.1 For vehicle tracking devices where the ARC is accredited in accordance with BS5979 (Cat II) and the systems in accordance with BS8484, a single URN will be allocated to the ARC in accordance with **Appendix U**

4.5 Police Attendance - Type B Security Systems

- 4.5.1 Type B alarm systems are described in paragraph 3.2.
- 4.5.2 To obtain Police attendance, Type B systems will require some additional indication from **a person at the scene** that a criminal offence is in progress which indicates that Police response is required. This will require human intervention such as member of public, owner or agent visiting, or viewing the premises. The addition of electronic means to provide confirmation will not promote such systems to Type A or achieve Police response.

- 4.5.3** Type B calls where there is additional information **from a person at the scene** that a crime is taking place should be passed to the Police by public telephone lines or 999 as appropriate. The level of Police response will depend on the quality of the information received and the Police operational requirements at the time of the 999 call.
- 4.5.4** Automatic dialling equipment must not be programmed to call Police telephone numbers.
- 4.5.5** Calls received from non-compliant ARCs/RVRCs/SOCs and calls from compliant ARCs/RVRCs without a valid URN will not receive a Police response unless circumstances outlined in 4.5.2 and 4.5.3 above applies.

5. LEGISLATIVE REQUIREMENTS

5.1 Data Protection Act 1998

- 5.1.1** Data supplied to the Chief Constable in relation to security systems may be held on a computer and Compliant Companies should notify their Clients that
- a) limited data supplied by them may be held on Police computers
- AND**
- b) where the data is relevant to a complaint, it may be disclosed to the UKAS accredited Inspectorate body recognised by the Police Service of Scotland.
- 5.1.2** Information supplied to the Chief Constable by Compliant Companies must be accurate and up to date. Any alterations to the personal data supplied by security companies must be notified to the Chief Constable within 14 days of the date of alteration.
- 5.1.3** Should any request be made in terms of subject access, the request will be dealt with in accordance with Part V of the Data Protection Act 1998.

5.2 European Court of Human Rights

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

5.3 Freedom of Information (Scotland) Act 2002

5.3.1 The Police Response to Security Systems Policy is publicly available and published on the Police Service of Scotland website ****new website address to be defined****.

5.3.2 Should any requests be received seeking further information about either the policy, its implementation, procedures used by the Police Service of Scotland or commercial organisation, or any other aspect, the request is to be dealt with by the Force Freedom of Information Officer.

5.4 Racial Equality

5.4.1 The policy has been drafted taking into account the appropriate principles of the Equality Act 2010.

5.5 Advertising

5.5.1 Security systems companies and ARC's shall not use terminology which might raise, in the mind of the customer, a guaranteed or unrealistic expectation of Police response to a security system and shall not use a Police Service of Scotland logo or reference in advertising material without written permission from Police Service of Scotland.

5.5.2 The use of wording inferring Police endorsement such as 'Police Approved', 'Police Preferred', 'Police Compliant' and 'Meets Police Requirements' must not be used.

5.5.3 Advertising material should not contain any references to recognised or compliant lists held by Police Service of Scotland or any other Police force. Photographic material or images of Police officers or vehicles must not be used.

6 UKAS CERTIFICATION BODIES AND RESPONSIBILITIES.

6.1 Certification Bodies and Requirements

UKAS Accredited Certification Bodies provide certification for a very wide range of products and services, and against a wide variety of standards and codes of practice. The certifying bodies can be found at **APPENDIX H** and the certification requirements can be found in **APPENDIX S**

7. POLICE REQUIREMENTS (Final Discretion)

7.1 Right of Refusal

The policy does not impose any liability on the Police Service of Scotland, its officers or employees or the Police Authority arising out of any acts or omissions connected with the security system installation, including failure or timeliness in responding to any activations. The Chief Constable reserves the right to:-

- a) refuse to admit a company to the compliant list.
- b) refuse to issue a Police URN for any installation.
- c) refuse Police response to any security system installation.
- d) to alter, amend or add to this policy as necessary

For specific operational reasons parts of this policy may not be applied to some URN's at the Force's discretion.

In addition, Police response to alarm activations will be dependent on the level of demand and resources available on receipt of a request for Police attendance to a system activation.

7.2 Policy Amendment Requests

Issues which may require amendment to this policy must be forwarded to the Data Processing Unit Command and Control Custodian, Elphinstone House, 65 West Regent Street, Glasgow, G2 2AF. The Custodian will discuss amendments with relevant organisations such as representatives of the British Security Industry Association (BSIA), UKAS accredited inspectorate bodies, the Insurance Representatives, etc.

7.3 Copyright

This policy is the copyright of the Association of Chief Police Officers in Scotland. This Policy is available on the Police Service of Scotland website ****to be defined****. Policies may be downloaded for individual use, but under no circumstances altered or amended.

INDEX TO APPENDICES

Appendix A	Policy variations to force service standard
Appendix B	Application to be accepted on Police list of compliant companies/policy agreement form
Appendix C	Disclosure of convictions
Appendix D	False alarm monitoring formula
Appendix E	Administration charges
Appendix F	Combined notice of intention to install and variation form / key to completion of Appendix F
Annexe A	Restoration of response to intruder alarm
Annexe B	Restoration of response to hold-up alarm
Appendix G	Hazards and site risk statement (health & safety)
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
<i>Appendices K-Q</i>	<i>Are advisory standard templates, for use by forces, if they so require.</i>
Appendix K	Police letter to customer on completion of installation
Appendix L	Notice of urn to installer
Appendix M	Letter to be forwarded to subscriber at three false calls
Appendix N	Letter from Police to customer advising withdrawal of Police response
Appendix O	Reinstatement of Police response letter
Appendix P	Deletion of unique reference number - letter to subscriber
Appendix Q	Deletion of unique reference number - letter to security system company
Appendix R	Requirements for companies installing and monitoring remote CCTV systems
Appendix S	Requirements for security systems services
Appendix T	Ten point plan for hold-up (personal attack) devices
Appendix U	Requirements for companies installing and monitoring after-theft systems with vehicle immobilisation for vehicle recovery
Annexe A	Police Service of Scotland vehicle tracking requirements
Annexe B	After theft vehicle immobilisation systems indemnity
Appendix V	Police requirements for lone worker services

Appendix A - Policy variations to Force service standard

As this policy relates to the Police Service of Scotland – any changes to the content of this policy will be include in the main body of the policy and not in this appendix. To align with the Association of Chief Police Officers (ACPO) policy this appendix is included although it will have no content

DRAFT FOR CONSULTATION

Appendix B - Application to be accepted on Police list of compliant companies/policy agreement form

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 Policy Compliant Security Companies.

Name of Home Force registered with.....

I have read the Police Service of Scotland Security Systems Policy and Requirements for Security Services. I agree to comply with every requirement of these documents.

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

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

..... *Position in Company*.....

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

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

This policy is a living document, which may be subject to amendment in April and October each year. It is your responsibility to ensure that your company is aware of these amendments. The policy is available on the Police Service of Scotland website (**to be defined****).**

Signature..... Print Full Name

Date.....

Address.....

.....Post Code.....

Telephone Number Fax number.....

Email for correspondence.....

Appendix B Continued

Our Alarm Receiving Centre(s)

(i) Name.....

Telephone Number
(for Police operational use)

(ii) Name.....

Telephone Number
(for Police operational use)

**Please Return to:- Police Service of Scotland Alarms Administration
Department, address *****to be defined******

Data Protection Act 1998

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

DRAFT FOR CONSULTATION

Appendix C - Disclosure of Convictions

This procedure will be entered into with companies on the List of Compliant Security System Installers of a Police Force or a company making a bona fide application for admittance to the List.

Unless other specific statutory requirements exist that are outside the scope of this Policy, employees will require to obtain a Disclosure Scotland 'Basic Disclosure' certificate which will contain details of convictions which are unspent according to the Rehabilitation of Offenders Act 1974.

From 1st April 2013, **new employees** of companies on a Force's List of Compliant Security System Installers will require to obtain a Basic Disclosure Certificate and provide it to that company prior to appointment. This requirement will apply to **current employees** of a company on the compliant list who will have until 1st April 2014 to comply with this requirement. Any new company applying for inclusion on the list of compliant companies will have to ensure that all relevant employees (detailed in item ii below) have obtained a Basic Disclosure Certificate or other acceptable documentation as described below.

In the case that a prospective employee has documentation issued within the preceding 12 months prior to employment date, proving:

- Disclosure Scotland Certificate or Enhanced Disclosure certificate,
- Criminal Records Bureau (CRB) Disclosure or Enhanced Disclosure Certificate,
- Access Northern Ireland Disclosure Certificate,
- or a specific force vetting certificate for approval for employment with the alarms systems industry,

then this will be accepted in lieu of a Basic Disclosure Certificate from Disclosure Scotland.

The intention is to curtail those with unspent criminal convictions (which can include theft, dishonesty, serious assault, the misuse of drugs, and offences of indecency) having access to premises and information relating to the security of premises.

PROPOSED PROCEDURE

A Disclosure Scotland Basic Disclosure Certificate must not take the place of normal recruitment procedures. References should be required and taken up in the case of all new appointments, with unexplained gaps in employment being satisfactorily accounted for in accordance with BS7858. Employers will need to ensure that they consider all information available to them from the Basic Disclosure Certificate or other acceptable documentation (as previously described) and references when considering the suitability of a prospective candida

Appendix C continued

- (i) Each applicant seeking employment where their duties will include surveying, sales, installation, maintenance, monitoring and administration of security systems with a company on a Force's List of Compliant Security System Installers, or a prospective company wishing to go on the List will have to ensure that a Basic Disclosure Certificate or equivalent recent (within last 12 months) Criminal Records Bureau, Access Northern Ireland Disclosure Certificate or Police check certificate has been obtained and can be evidenced.
- (ii) Employers may wish to make a statement available to people who may be subject to these arrangements, to reassure them that ex-offenders will not automatically be rejected.
- (iii) When a Basic Disclosure Certificate is required, the employer should ask the potential employee for permission to submit an application for a Basic Disclosure to Disclosure Scotland (unless they have evidence of a relevant CRB, Access Northern Ireland or ACPO Police check within the last 12 months).
- (iv) Employers must be satisfied as to the identity of the applicant prior to the submission of the application for a Basic Disclosure Certificate and retain written record of how this was undertaken. They must also confirm the correct spelling of the full name, the date and place of birth, current address and all other information required on the application form.
- (v) Where a person wishes to complain about the Disclosure on the grounds they have been incorrectly identified or any information contained therein is incorrect, they should have an opportunity to make representations. This should be done in the first instance through the employer who requested the Disclosure Certificate.
- (vi) In the event of a requirement to obtain a Disclosure Scotland basic Disclosure Certificate from a foreign national, the application will also require an attachment of the relevant overseas criminal record check; this will need a form of authentication and be translated into English. For further guidance refer to the [Overseas Criminal Records Check](#) section of the [Security Industry Authority](#) website.

Appendix C continued

- (vii) In the event of a British Citizen having worked outside of the UK for a period in excess of six continuous months in the last 5 years, they will also be required to provide an overseas criminal record check.
- (viii) 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 accredited list for non-compliance with this policy.
- (ix) 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.

DRAFT FOR CONSULTATION

Appendix D - False alarm monitoring formula

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

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

a = the force false alarm rate for a particular reference period (e.g. 28 days, month or year)

N = the number of installations for a particular company

Z = the value taken from tables based on normal distribution. The figure of 1.64 has been chosen to give the following producers risk and consumer's risk.

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

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

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

Mode of application

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

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

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

- 1) Where a claim is made that the upper action level has been exceeded on the grounds of unique types of alarm installations a revised rate may be introduced at the discretion of the Chief Constable. Where the Chief Constable considers a claim for a revised upper action level is unacceptable he may refer the matter to the appropriate independent inspectorate for arbitration.

Appendix D continued

- 2) Where a reduction to the false alarm rate is not achieved within a three month period the Chief Constable will consider the following options-

if the company appears to have made little or no effort to resolve the problem an immediate withdrawal of facilities to acquire new unique reference numbers (URNs) will take place until the company has reduced their false alarm rate to within their upper action level. The circumstances will be reported to the appropriate inspectorate body as a serious non-compliance with the Police Service of Scotland Requirements for Security Systems Services document.

or

if the company demonstrates it has tried but been unsuccessful in reducing their false alarm rate to within their upper action level the circumstances will be reported to the appropriate inspectorate body as a non-compliance. Chief Constable may agree objectives with the company to resolve the matter, in such cases the URN facility will not be withdrawn.

Appendix E - Administration Charges

The following charging structure is adopted by the Police Service of Scotland to recover administration costs in respect of security systems. Payment shall be made to the Police Service of Scotland Alarms Administration Department dealing with the alarms administration for the relevant area.

1. Each application for a URN is subject to an administration fee payable by the system user. **The URN Fee is £43.49 plus VAT** and will be reviewed every year by Police Service of Scotland. (See Appendices U & V for vehicle tracking and lone worker systems).
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 informed.
3. The administration fee is payable for:
 - a) New URN applications
 - b) New occupiers/owners of premises taking over existing security systems (system retains false alarm history unless upgraded to DD243 2004)
 - c) Existing user changing security company (system retains false alarm history unless upgraded to DD243 2004)
Where a security company cancels a URN, a period of 28 days grace should be given to allow another security company to takeover the URN before it is deleted.
Where a security company applies to takeover a URN from an existing company and/or Maintenance Contract, they may do so supported by the customer's authority.
4. The administration fee is not applicable when:
 - a) A security company takes over another security company.
 - b) A security company ceases to trade and another company takes over the URNs within 28 days of the company ceasing trading.
 - c) Premises change name only (Evidence will be required to ensure it is a change of name only and not change of owner/user)
Systems will retain their false alarm history unless upgraded to DD243:2004
5. In the event the installation does not proceed after the URN has been allocated, the fee is non-returnable
6. All security system monitoring centres operating under this policy must utilise the dedicated ex-directory lines, or specified electronic data transfer method nominated by the Police Service of Scotland. An access fee may be chargeable and will be recovered by either a) the use of premium rate

Appendix E continued

telephone call charges or b) an annual fee. If this applies it will be detailed in section 3.1 under TYPE A systems.

7. If caller line identification is operated, central stations must not bar this facility on Police calls.
8. A stamped, addressed envelope (SAE) is required with all mailed URN applications.

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

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

******NOTE – ACPO is currently reviewing this appendix. Proposed amendments are not yet reflected in the draft Police Service of Scotland policy, but may be included in a future version subject to separate consultation.*****

POLICE SERVICE OF SCOTLAND POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS

NOTICE OF:

VARIATION REASON(S):

		Installation Date:	
		Variation Date:	

INT URN	1	
P/A URN	2	
URN	3	

NAME OF ALARM RECEIVING CENTRE
Police Ref:
Address
Tel:

NAME OF INSTALLER
Police Ref:
Address
Tel:

NAME OF MAINTAINER
Police Ref:
Address
Tel:

DETAILS OF PROTECTED PREMISES

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

TYPE OF SYSTEM

TYPE OF CONFIRMATION

ADDITIONAL FEATURES

GRADE OF SYSTEM

STANDARD TO WHICH INSTALLED

EXISTING URN NO.			
Int		CCTV	
H-UP		Veh tracking	

PREVIOUS USER (Company name when applicable)

ADMIN FEE	SOUNDER DELAY

CERTIFICATE /Contract no	
---------------------------------	--

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

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

POLICE USE ONLY

DRAFT

PSoS SECURITY SYSTEMS POLICY

APPENDIX F KEY

KEY TO COMPLETION OF APPENDIX F DOCUMENT

Select the type of notice, from 1 to 3.

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

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

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

TYPE OF SYSTEM (1)	TYPE OF CONFIRMATION (1 2 3)	ADDITIONAL FEATURES (1 2 3)	Grade of System (1 2 3)
Intruder Alarm	Audio	None	Grade 2
Hold Up	Visual	Smoke Generator	Grade 3
Combined IA/H-UP	Sequential	CCTV	Grade 4
CCTV	Audio and Sequential	Lighting	
Vehicle tracking	Visual and Sequential	Chemical trace	
Lone Worker	Visual and Audio	Access control	
CAT 5	Visual, Audio and Sequential	Smoke Raid Control (H-UP)	
ADMIN FEE (1 2 3)	STANDARD TO WHICH INSTALLED (1)	TYPE OF PREMISES (1)	VARIATION REASON(s) (1 2 3)
Applicable	BS 4737	Retail	Upgrade to confirmation
Not Applicable	PD6662 2004 + DD243 2004	Commercial	Signalling amendment
	PD6662 2010 + BS8243	Public Sector	New user
	BS 4737 + DD: 243:2002	Licensed	Change of user name
	BS 4737 + DD243 : 2004	Domestic	Address amendment
	BS 6799 Class VI	Industrial	Additional features
	BS7042	Bank or Financial	Takeover from another maintainer
0 Minutes	BS8418 2003	Institutional	Change of Alarm Receiving Centre
5 Minutes	BS8418 2010	Other	Maintenance contract cancelled
10 Minutes	BS 8484		System removed
15 Minutes	Cat 5 ATSVIVR		Change of sounder delay

Appendix F Annexe A - Application for restoration of Police response to an intruder alarm

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

N.B. Although withdrawal of response will not in the short term affect the status of the hold-up (personal attack) alarm, please note that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated to your Intruder / PA will be deleted. It is therefore essential that you give this matter your urgent attention.

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

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

CURRENT STATUS	REQUIREMENT	COMPLETED (√)
1) Pre DD243 system	Upgrade to DD243:2004 or BS8243	<input type="checkbox"/>
2) DD243 system pre 2002	Upgrade to DD243:2004 or BS8243	<input type="checkbox"/>

Please note remedial action in 1 & 2 above could lead to reinstatement of response - without a 3 month delay.

3) DD243:2002 system	Identify cause, remedy, and detail remedial action in box below	<input type="checkbox"/>
4) DD243:2004 system	Identify cause, remedy, and detail remedial action in box below	<input type="checkbox"/>
5) PD6662 2010	Identify cause, remedy, and detail remedial action in box below	<input type="checkbox"/>

*Please note that systems in 3 & 4 above must have been free of false calls for a continuous period of 3 months (supported by ARC evidence) **BEFORE** this application for restoration is submitted.*

There is no requirement to upgrade to PD6662 to regain Police response

Appendix F – Annexe A continued

Identify the cause of the false alarms and give details of remedial work carried out in the box below (supported by evidence, such as an engineers report sheet)

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.

Signed:.....Date:.....

Name:.....(please print)

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

Appendix F Annexe B - 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.

Although withdrawal of response will not in the short term affect the status of the intruder alarm, please note that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated to your Intruder / Hold-up will be deleted. It is therefore essential that you give this matter your urgent attention.

URN	NAME & ADDRESS OF PREMISES	INSTALLER / MAINTAINER

- 1) Is a Police response still required for the Hold-up facility? **YES / NO**
- If not, have appropriate measures been put in place to ensure that signals are not passed to the Police? (you may need to consult your insurance company, if the device has been removed). **YES / NO**
- 2) Confirmation is mandatory – is this in place? **YES/NO**

When a form of confirmation has been implemented for the first time, response may be reinstated to Hold-up alarm before the 3 month period.

Any subsequent Level 3 loss of response, *after confirmation has been put in place*, a system must achieve three months' clear of false calls.

If the method of hold-up confirmation is not filtering out false calls effectively, the Police reserve the right to request that one of the alternative methods are used.

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 confirmation, the purchasing contractor or other person responsible for health and safety under applicable legislation must ensure adequate support systems are

Appendix F – Annexe B continued

in place within 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.

Please explain the method of confirmation used in this box, e.g. ‘call-back’, ‘visual’, ‘audio’, ‘ sequential’ or ‘any combination’.

- 3) Has the system been clear of false calls for three months? **YES / NO**
(If applicable*)
- 4) Are all of the hold-up devices dual action? **YES/NO**
- 5) Has the Duress facility been removed? **YES/NO**
(Only BS EN 50131-1 Grade 4 (Grade 3 in exceptional circumstances) & BS 7042 systems are exempt from this requirement).
- 6) Has user training been given? **YES/NO**
- 7) Does Hold-up alarm comply with all other aspects of **Appendix T** 10-point plan? **YES/NO**

Give details of cause and any other work undertaken to rectify false Hold-up alarms in this box.

Appendix F - Annexe B continued

I declare the End User(s) have been fully trained in the confirmation method and procedures to be followed in the event of the Hold-up alarm being activated. (A record of training is to be kept available for inspection by the Police or inspectorate bodies)

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

Signed:.....

Date:.....

Name:..... (please print)

Position in Company.....

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

DRAFT FOR CONSULTATION

Appendix G - Hazards and site risk statement (Health & Safety)

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

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

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

MY SECURITY SYSTEMS COMPANY NAME IS:
The following applies to the building(s) and grounds of these premises:

	✓		✓
POND	<input type="checkbox"/>	DOGS	<input type="checkbox"/>
SWIMMING POOL	<input type="checkbox"/>	DANGEROUS ANIMALS	<input type="checkbox"/>
RIVER FRONTAGE	<input type="checkbox"/>	FIREARMS	<input type="checkbox"/>
GLASS COPING WALLS	<input type="checkbox"/>	AMMUNITIONS	<input type="checkbox"/>
RAZOR WIRE	<input type="checkbox"/>	EXPLOSIVES	<input type="checkbox"/>
INSPECTION PITS	<input type="checkbox"/>	DANGEROUS MACHINERY	<input type="checkbox"/>
SETTLEMENT TANKS	<input type="checkbox"/>	GAS CYLINDERS	<input type="checkbox"/>
VATS	<input type="checkbox"/>	TOXIC MATERIALS	<input type="checkbox"/>
BASEMENT	<input type="checkbox"/>	CONTAGIOUS SAMPLES	<input type="checkbox"/>
FRAGILE ROOF	<input type="checkbox"/>	FLAMMABLE SUBSTANCES	<input type="checkbox"/>
DANGEROUS STRUCTURE	<input type="checkbox"/>	FUEL STORAGE	<input type="checkbox"/>
LOW CEILING BEAMS	<input type="checkbox"/>	CHEMICALS	<input type="checkbox"/>
SLIPPERY FLOORS	<input type="checkbox"/>	RADIO ACTIVE MATERIALS	<input type="checkbox"/>
FURNACE	<input type="checkbox"/>	ASBESTOS	<input type="checkbox"/>
ELECTRICITY SUB-STATION	<input type="checkbox"/>	SPRINKLER SYSTEM	<input type="checkbox"/>
ATM <i>INSIDE PREMISES</i>	<input type="checkbox"/>	SECURITY FOGGING DEVICE	<input type="checkbox"/>
SMOKE RAID CONTROL (HOLD-UP)	<input type="checkbox"/>		

OTHERS:

Appendix G continued

IF NO SITE HAZARDS OR RISKS, STATE NONE:

--

The Following is confirmed

1. Alarm Receiving Centre has been given details of two key holders capable of attending within 20 minutes of notification. The user is aware that persistent failure unjustifiably of key holders to attend within that time may result in the withdrawal of Police response and/or approval for the system.

The system user irrevocably authorises the system installer/maintainer/security systems company, the security systems company) at their own discretion to pay to the Police the URN administration fee on his/her behalf and accepts, notwithstanding this, that the liability for the payment of the fee rests solely with the user, that the security company cannot be held liable in any way if it does not pay the fee and agrees to indemnify the security company against any financial liability incurred in connection with the payment of the URN fee.

2. The system user agrees that nothing in this or any other agreement shall constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the parties or between the security company and the Police.
3. The system user acknowledges that the payment of the URN administration fee does not imply any assurance that a URN will be provided by the Police and the provision of a URN does not imply or guarantee any service or response from the Police will be provided.

Name of Occupier / Premises			
Address			
County		Postcode	
Telephone Number			

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

If commercial business;

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

Appendix G continued

POLICE ADMINISTRATION FEE £43.49 + VAT (if applicable) MUST BE ENCLOSED WITH THIS FORM AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY– CHEQUES/POSTAL ORDERS SHOULD BE MADE PAYABLE TO YOUR POLICE SERVICE OF SCOTLAND ALARMS ADMINISTRATION DEPARTMENT. PLEASE DO NOT SEND CASH

Should site hazards and risk circumstances change you must update our records (free of charge).

Data Protection Act 1998

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

Appendix H - Police advice to members of the public seeking information on security companies

To obtain information on companies who supply and install security systems such as Intruder Alarms / hold-up (Personal Attack) 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 and 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 themselves are governed by UKAS (United Kingdom Accreditation Service), the sole accreditation service recognised by the Government.

Please note - if you are also planning to invest in the type of security system that would receive *automatic Police response* to its alarm activations, then only security companies 'Approved' by an Independent Inspectorate Body and who are Listed with the Police Service of Scotland 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, compliant with the Police Service of Scotland Security Systems Policy, we advise: -

- (a) Before disclosing personal security details, check the address and credentials of the company and proof of identity from their representative.
- (b) You obtain written quotations from at least two 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 Service of Scotland, for the transmission of alarm activations from new installations?
- (d) You ensure that the quotation specifies that the installation will be to European/British Standards for that relevant security system. Also, does it include the terms of maintenance and monitoring contracts?
- (e) Does the company operate a 24-hour call-out service and emergency attendance within four hours?
- (f) Is the installation of a security system a requirement of my insurance company and if so, is the security company acceptable to my insurer?

Appendix H continued

PLEASE NOTE - When investing in Security Systems for your home or business it's 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, 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 this type of security company, they should contact the Police or Trading Standards for advice.

For further information on intruder alarm advice for domestic properties visit www.securedbydesign.com and www.consumerdirect.gov.uk/watch

DRAFT FOR CONSULTATION

Appendix I - Letter to be handed to potential customers by all companies installing security systems

Dear Sir/Madam

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

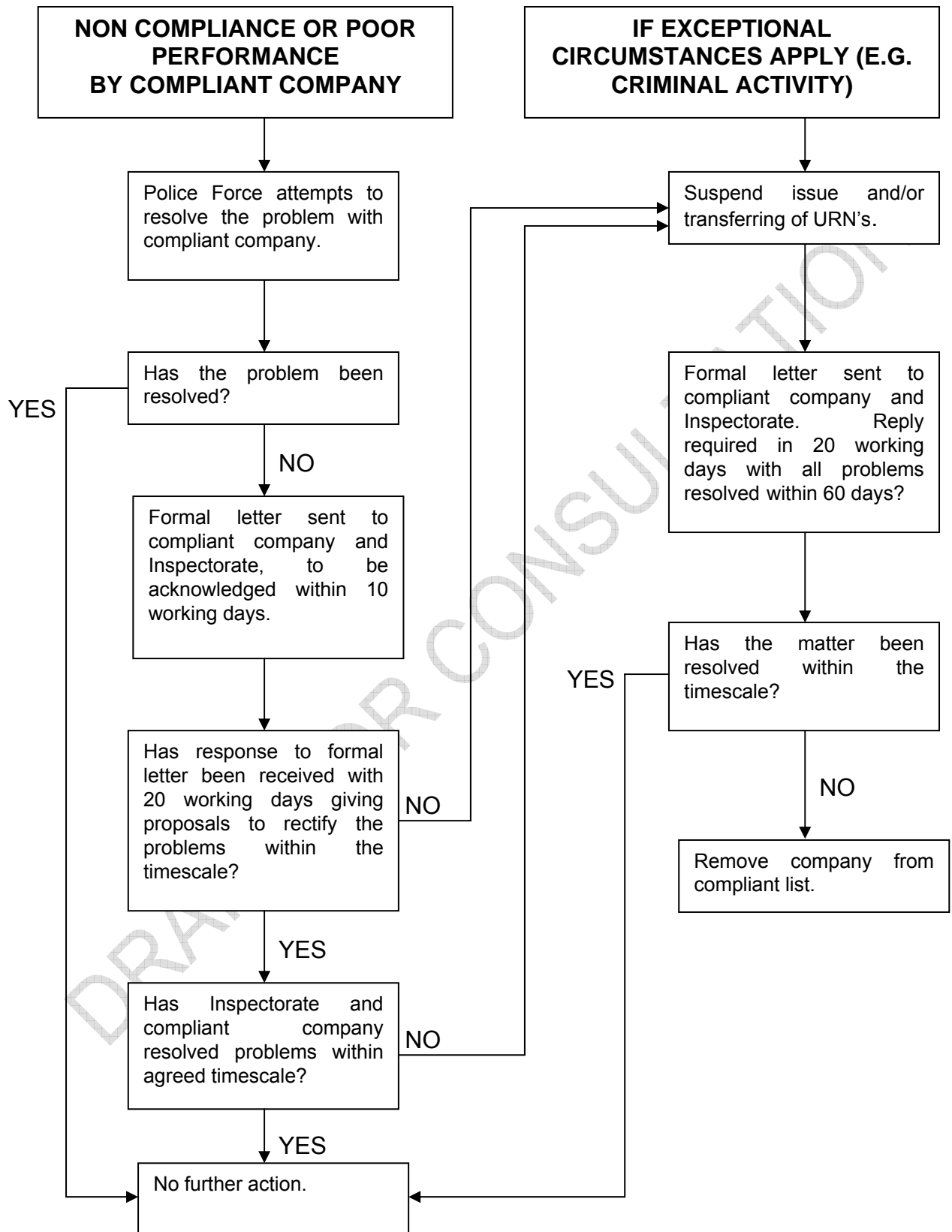
To avoid misunderstanding, here is a précis of the conditions. However, should you require further information please contact your local crime prevention / community Police officer.

1. Installation, maintenance and monitoring of security systems must only be undertaken by companies acceptable to your local Police.
2. Such acceptance by the Police does not imply guarantee of the company's work. You should seek confirmation from the company that it is compliant with Police policy and is acceptable for the transmission of alarm messages from new installations.
3. You will receive training on the operation of the system by the installer including methods of cancelling accidental operations of the alarm.
4. Commercial premises may be required to have a 10 minute delay of sounders to give us the opportunity to attend and detain offenders. You may apply to Police Headquarters for exemption to the delay.
5. Any external audible sounder should cut out after 20 minutes and alarms causing annoyance under the terms of the Control of Pollution Act 1974 and Environmental Protection Act 1990 may result in prosecution.
6. Security systems will receive a Police response determined by the nature of demand, priorities and resources which exist at the time. To maintain the efficiency and prevent avoidable Police deployments, alarm system performance including false alarm activations will be closely monitored. Currently, UK Police alarm policies related to false alarm activations are being standardised. As a result the following position will commence from **2013**.
 - a) From 1st April 2013, security systems will receive an immediate response – subject to other urgent Police incidents (**level 1** response) until three false calls have been received in a rolling 12 month period. The security system will drop to a **level 2** response (Police attendance desirable subject to available resources). If two more false calls are made in a 12 month rolling period then the security system will drop to a **level 3** response (no automatic Police response without other evidence of criminality).

Appendix I continued

- b) On **1st April 2014** security systems will receive a **level 1** response until 2 false calls are recorded. Police response will then drop to a **level 2** and following one more false alarm, the system will drop to a **level 3** response.
7. 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 within 6 months of withdrawal of Police response otherwise the URN will be deleted. It is therefore in your interest to identify and correct the cause of any false alarm at the earliest opportunity.
8. 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.
9. There is a requirement to have at least two key holders, details of whom will be maintained by the Alarm Receiving Centre. Key holders 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.
10. In accordance with the Data Protection Act 1998 personal information relating to you and your key holders in connection with the security system may be held on a computer. Please ensure that relevant names and addresses are current. It is regretted that such constraints are imposed but they are essential if we are to maintain the credibility of alarm systems, reduce false calls and provide you with an acceptable service.

Appendix J - Memorandum of understanding



Appendix K - Police letter to customer on completion of installation

Dear Sir/Madam,

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

You are advised that Police personnel may have to be withdrawn from the premises before the arrival of a key holder. In this case the key holder 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 formulated the following policy:

Every user having a system which produces three false calls (*from 1st April 2013 to 31st March 2014 or two false calls thereafter*) within a period of 12 months, shall be served with a notice requiring action to be taken to prevent further false calls.

Should five false calls (*from 1st April 2013 to 31st March 2014 or three calls thereafter*) be received within any 12 month period, Police response will be withdrawn. Response may be reinstated if remedial action has been taken to rectify the fault, or when the system has achieved three months free of false calls within 6 months of withdrawal of Police response otherwise the URN will be deleted.

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

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

2. KEYHOLDERS

You should provide your alarm company with at least two key holders 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.

3. NOISE NUISANCE

Appendix K continued

Any external audible sounder should cut out after 20 minutes and alarms causing annoyance under the terms of the Control of Pollution Act 1974 and Environmental Protection Act 1990 may result in prosecution.

4. HOLD UP (PERSONAL ATTACK) ALARMS

The Security Systems Policy states “A personal attack may be operated to summon urgent Police assistance when a person is threatened with immediate personal violence or criminal act”. However in many instances hold-up alarms are used where there is no threat to persons within a defined area. Without knowing the circumstances under which the hold-up alarms are activated, the Police must respond. You should be aware that in the current policy, if you use the Hold-up alarm twice within a rolling twelve month period and there is no threat to persons in a defined area, you will lose Police response for a period of time.

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

Accidental misuse of your Hold-up system could cause you to lose Police response. Guard against this possibility.

The following are examples of intentional but non-essential operation of a Hold-up alarm 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 Hold-up alarm is there to summon Police assistance when you are threatened. DO NOT use it for any other purpose.

5. DATA PROTECTION ACT 1998

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

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

Yours faithfully,

Appendix L - Notice of URN to installer

Dear Sir/Madam,

RE: _____

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

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

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

It is a requirement of the _____ Police that all security systems installed should meet the British Standard BS EN 50131-1 (PD 6662 scheme for the implementation of European Standards), BS 4737, BS 7042, BS 6799 or BS 8418 and Codes of Practice identified in the Policy and that the installing company issue a certificate to that effect.

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

Yours faithfully,

Appendix M - Letter from the Police to customer at three false calls

(from 1st April 2013 to 31st March 2014 – thereafter TWO false calls)

Dear Sir/Madam,

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

In an effort to reduce the unacceptably high number of false calls received by the Police, it has been necessary to introduce a policy governing the installation, maintenance, monitoring and use of security systems. The policy includes a close monitoring of all calls. Records indicate that there appears to have been at least three (two from 1st April 2014) false calls from the system at your premises within a twelve-month period. In view of this, you are advised to contact your security systems company at the earliest opportunity in an effort to resolve what appears to be a problem with your security system or its operation.

Regrettably, should you have a total of five (three from 1st April 2014) false calls within a rolling twelve month period, it will be necessary to consider the withdrawal of Police response to activations from your system, a situation we would wish to avoid with your co-operation.

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

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

Yours faithfully,

Copy to: Security System Company

Appendix N - Letter from Police to customer advising withdrawal of response

Dear Sir/Madam,

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

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

Following careful consideration I have to inform you that Police response will no longer be given to your security system after the _____. Reinstatement of response can be considered following notification from your security company that your system has been upgraded if required, or remedial action has been taken to rectify the false calls and a period of three months free of false calls has been achieved within 6 months of withdrawal of Police response otherwise the URN will be deleted. 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.

Yours faithfully,

Copy to: Security System Company

Appendix O - Letter from Police to customer reinstating Police response

Dear Sir/Madam,

RE: _____

Further to correspondence received from your alarm maintainer requesting re-instatement of response dated _____, this 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.

It should be noted that the Police will continue to monitor false calls from your premises and should five false activations (three from 1st April 2014) be accrued within a rolling twelve month period, consideration will be given to withdrawal of Police response.

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

Yours faithfully,

Appendix P - Letter from Police to customer on deletion of unique reference number

Dear Sir/Madam,

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

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

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

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

Yours faithfully,

DRAFT FOR CONSULTATION

Appendix Q - Letter from Police to security system company on deletion of unique reference number

Dear Sir,

RE: _____

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

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

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

Yours faithfully,

DRAFT FOR CONSULTATION

Appendix R - Requirements for companies installing and monitoring remote CCTV systems

1. INTRODUCTION

- 1.1** This document sets out the Police requirements for remotely monitored detector activated CCTV systems to enable such systems to apply for URNs from the Police Service of Scotland.
- 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 this policy, will be known as Type A systems and will be issued with a URN.
- 1.4** Systems for which Police attendance may be required and which operate outside the procedures identified in the policy, 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 Service of Scotland Security Systems Policy clause 4.1.

2. STANDARDS

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

Appendix R continued

3. LEGAL REQUIREMENTS

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

4. PROCEDURES

- 4.1 The Police Service of Scotland will be sent a notice of installation of a remotely monitored detector activated CCTV system using Appendix F of the Police Service of Scotland Security Systems Policy. A URN will be issued for the appropriate fee (as outlined in appendix V) in line with the relevant this Policy.
- 4.2 The means of image collection and communication between the premises and the RVRC is a matter for the installer and the RVRC. However, the system will be installed to meet the requirements of Clause 2 of this appendix.
- 4.3 The system will be maintained in accordance with the BS 8418 (Clause 13.1), and the requirements of the Data Protection Act 1998, CCTV Code of Practice (latest edition).
- 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, or the activity gives cause to suspect that there is intent to commit a crime.
- 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 the Police Service of Scotland for investigative purposes will be supplied upon request.

Appendix R continued

- 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.

RVRCs using digital recording methods will adhere to the procedures for processing digital images, issued jointly by the Home Office, ACPO and Police Scientific Development Branch.

5. MANAGEMENT INFORMATION

- 5.1** RVRCs will provide management information that is compatible to Police Service of Scotland in relationship with the systems for analysis.
- 5.2** The information supplied will give a detailed analysis of the total number of calls passed to the Police, registered with the URN.
- 5.3** Remotely monitored detector activated CCTV systems will be subject to the same conditions as laid down in the Police Service of Scotland Security Systems Policy (Section 4 refers) in relation to the total number of incidents incorrectly passed to the Police.
- 5.4** The Memorandum of Understanding (MOU) appendix J is applicable to CCTV systems.

6. INDEMNITY

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

Appendix S - Requirements for security system services

- I For the issue of a URN by the Police Service of Scotland, the installation / services provided by the Installation, Maintenance or Monitoring Company shall be certified in accordance with the provisions of this document by a certification body accredited to EN 45011 by United Kingdom Accreditation Service.
- II The Certification Body shall -
- a. Be a company limited by guarantee and not having a share capital. The company is to be formed in accordance with the relevant Companies Act identified in Appendix S 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 Appendix S Annexe A or suitable individuals.
 - c. Ensure the memorandum and articles of association and their company law members/guarantors are specific to a certification body and identify the objects of a properly constituted certification body.
 - d. Provide audited accounts, where applicable, or such other accounts as are mandatory under Company Law, to show compliance with Clause 4.2(i) BS EN 45011: 1998
 - e. Carry out surveillance of certified service providers in accordance with the provisions of paragraph III. Surveillance shall be conducted at a minimum frequency of once per year and for installation companies, this surveillance shall include an inspection/functional test of installation(s) for compliance with the appropriate documents identified in Appendix S Annexe A
 - f. Have documented procedures for the inspection and test of installed and maintained systems to ensure compliance with the appropriate documents identified in Appendix S Annexe A.
 - g. Ensure personnel who have access to third party security arrangements as a result of this process shall be subject to a security vetting procedure to British Standard 7858 or an equivalent, which identifies any unspent convictions or associations, which may be deemed unacceptable.
 - h. Be required to establish if certification has been given and/or withdrawn by any other Certification Body accredited to this scheme when an Installation, Maintenance or Monitoring Company makes application for acceptance.

Appendix S continued

- i. Where disciplinary action is pending, in process or has resulted in expulsion by Certification Body 'A' of an Installation, Maintenance or Monitoring Company, for non-compliance with documents identified in Appendix S 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 the Police Service of Scotland with the Memorandum of Understanding (Appendix J).
- III Installing, Maintaining and/or Monitoring Companies

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

- a. Vet personnel who have access to third party security arrangements in accordance with British Standard 7858, which ensures personnel of good repute and identifies any unspent convictions or associations which may be deemed unacceptable.
- b. Trade Lawfully
- c. Have financial stability to trade, at present and in the future.
Guidance - The certification body in determining financial stability to trade, may consider checking bank references, court orders and annual accounts prepared by an independent accountant, i.e. as provided to the Inland Revenue. In the case of an incorporated company the audited annual accounts or such accounts as are statutorily required should a company be exempt from audit.
- d. Have adequate and relevant insurance in respect of employers, product, public, efficacy and wrongful advice liability.
Guidance - Insurance cover to a minimum of £1,000,000 per incident.
- e. Have competent management with responsibility for all services provided.
Guidance – Management must be conversant with the relevant standards for the services they provide and be competent to inspect and test systems. Their responsibility extends to services provided by sub-contractors who must comply with all aspects of this document.

Appendix S continued

- f. 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.
- g. Have adequate arrangements, documented procedures and systems in place for all of their activities.
*Guidance – This covers all aspects of a company's installing, maintaining and monitoring activities and includes –
Personnel (includes vetting, competence, qualification)
Sales (includes enquiry, survey, quotation, order)
Installation (includes design planning, commissioning, and training of subscribers)
Maintenance (includes preventative and corrective)
System performance
Confidentiality
Handling of system activations .e.g. intruder alarm filtering
Complaint handling
The documented procedures are to the extent necessary to achieve consistency of application.
Complaint handling needs to show logging, corrective action and review procedures.*
- h. Have suitable premises where confidentiality can be maintained and with adequate safeguards for security of information on a 24 hour basis.
Guidance – Any means of electronic security protection used for this purpose shall comply with the minimum standards of these procedures. Alarm receiving centres and/or monitoring centres must comply with the appropriate standards in Annexe A.
- i. 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.
- j. Have sufficient systems installed and/or monitored to enable competence and trading history to be determined.
- k. Have immediate access to and comply with standards and documents identified in Annexe A.

Appendix S continued

- I. Have customer contracts describing the products and services to be supplied together with the associated terms and conditions. *They are to be fair and reasonable, describe the products and services to be provided, show title to any equipment, describe the terms of the warranty and detail **all** the charges applicable.*
 - m. Not engage in pressurised selling or unfair business ethics.
- IV As new standards and documents become applicable to this scheme, Police Service of Scotland Security Systems Group will notify all Certification Bodies accredited to this scheme.
- V Where amendments to this scheme are deemed appropriate by the Police Service of Scotland, consultation will be instigated with those concerned.

Appendix S Annexe A - British Standards and European Norms

(Current issue unless stated – see notes 1 & 2)

BS 4737	Intruder Alarms in Buildings (mostly withdrawn see note 2)
BS 7042	High Security (withdrawn see note 2)
BS 8418:2010	Remotely monitored detector activated CCTV Systems
BS 8418:2003	Remains acceptable for new systems until 31 July 2011 (note 1)
BS 5979	Alarm Receiving Centres (Category II)
BS 6799	Wire free Alarms (withdrawn see note 2)
BS 7858	Security screening of individuals employed in a security environment
PD 6662:2010	Scheme for the application of European Standards for intruder and hold-up Alarm systems.
PD 6662:2004	Remains acceptable for new systems until 31 May 2012 (note 1) (Attention is drawn to BSIA Form 171 - Guidance Notes)
BS EN 50131 series	Intruder & Hold up Alarms
BS EN 50132-7	Alarm systems – CCTV surveillance systems used in security applications – Application guidelines
BS EN 50136 series	Alarm Transmission systems
BS EN 50131-8	Smoke Security Devices (applies under PD6662:2010 – note 1)
BS 8473	Management of False Alarms
BS 8243	Installation & configuration of Intruder & HUAs designed to generate confirmed alarm systems (applies under PD6662:2010 – note 1)
BS8484	Provision of Lone Worker Device Services

Appendix S (Annexe A contd)

British Standard Institution Drafts for Development (Latest Issue)

BS DD 242	High Security (withdrawn see note 2)
BS DD 243	Applies under PD6662:2004 (note 1)
BS DD 244	Wire Free Alarms (withdrawn see note 2)
BS DD263	Alarms Systems Commissioning, Maintenance and remote support (applies Under PD6662:2010 see note 1)
DD CLC/ TS 50131-7	:2008 Alarm Systems – Intrusion Systems – Application Guidelines
DD CLC/ TS 50131-7	:2003 Applies under PD6662:2004 (note 1)

Notes

1. Certain standards are in a period of “Duel running” with previous issues, and either current OR the previous issue may be acceptable for a specified, limited period.
2. Certain older and withdrawn standards or parts of standards are still included in this list for the benefit of legacy systems that remain in service.

Vehicle Tracking

Category 5	Criteria for System Operating Centres June 2010
Category 5	Criteria for original Equipment Manufacturers
ACPO & Centre for Applied Science & Technology (CAST)	HOSB 14/02 Stolen Vehicle Tracking

CEN TS 15213 series	Road transport & traffic telematics - After theft systems for recovery of stolen vehicles
---------------------	---

Legislation

The Control of Pollution Act 1974 and Environmental Protection Act 1990 **set out requirements for intruder alarms, key holders and noise.**

The Companies Act 1985 and 1989

Appendix T - Ten point plan for hold-up (personal attack) alarms

1) FILTERING

The ARC's are not in a position to pass only confirmed Hold-up alarms to the Police. The fact that someone does not answer the telephone does not confirm the activation is genuine as access to the telephone may be restricted, or that staff are too busy to answer it. In the event of the telephone being answered an operator is not always in a position to determine from what is (or is not) heard, if the activation is genuine.

However, where the ARC's are in a position to attempt to filter unwanted false activations through some form of agreed confirmation process, false calls will be reduced.

2) WITHDRAWAL OF POLICE RESPONSE

Hold-up alarm Police response levels and false activation monitoring will be consistent with that of Type A systems as outlined at Section 4 of this policy.

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

When a form of confirmation has been implemented, Police response may be reinstated to Hold-up alarm before the 3 month period. Any subsequent loss of response, after confirmation has been put in place, a system must achieve three consecutive months free of false calls supported by evidence from the security company.

3) HOLD-UP SYSTEMS ON Contact Identification Equipment (CIE) or Ancillary Control Equipment (ACE) SHOULD BE SEGREGATED FROM THE MAIN KEYS, DEDICATED, DEFINED AND ARE 2 SEPARATE BUTTONS SYNCHRONISED PUSH.

4) HOLD-UP SYSTEMS ON CIE OR ACE SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. This will stop the Hold-up alarm signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

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

The logic of restricting duress codes to high security systems to ensure that the risk warrants the facility. Inadvertent use of the duress codes from the CIE lead to a significant abuse of Police resources.

Appendix T continued

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

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

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

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. The purpose of this software change is to ensure that the duress facility is restricted to BS 7042 and EN 50131 grade 4 systems (Grade 3 in exceptional circumstances) and not customer programmable. This will stop the duress signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

7) **NO SINGLE ACTION 'SINGLE PUSH' HOLD-UP DEVICES SHOULD BE ALLOWED**

Only 2 separate buttons with synchronised push systems should be allowed, as this would stop accidental activation by people 'bumping' against the Hold-up alarm. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' Hold-up devices in the event of losing Police response.

8) **NO TIME DELAY DEVICES ARE TO BE ALLOWED**

In these types of systems the Hold-up alarm is pressed once to start a timer. The occupier can then answer a door, check for intruders etc. If the Hold-up is not pressed a second time, the timer will time out and the Hold-up alarm is sent. This type of arrangement is a recipe for false alarms and will need to be redesigned in the event of losing Police response.

9) **PORTABLE HOLD-UP DEVICES (WIRELESS DEVICES) SHOULD BE DEDICATED AND NOT INCORPORATE ANY OTHER FUNCTIONALITY AND SHOULD HAVE 2 SEPARATE BUTTONS, SYNCHRONISE PUSH TO ACTIVATE**

This requirement is to stop single button type alarms, e.g. care alarm type systems being used as hold-up alarms. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' wireless devices in the event of losing Police response.

Appendix T continued

10) TRAINING / RE-TRAINING OF USERS

The training or re-training of users should be incorporated into the maintenance. The user should also be made responsible for the training of their key holder and this should be documented with the maintenance report.

Documentation should be provided to indicate when to use and when not to use a hold-up (personal attack) device. The key holder should be made aware of the serious implications of misuse.

DRAFT FOR CONSULTATION

Appendix U - Requirements for companies installing and monitoring after-theft systems with vehicle immobilisation for vehicle recovery

1. INTRODUCTION

- 1.1** This appendix sets out the Police requirements for the installation and monitoring of After Theft Systems with Vehicle Immobilisation for Vehicle Recovery (ATSVIVR).
- 1.2 Only qualified and registered personnel who meet these Police requirements can install ATSVIVR systems.**
- 1.3** Systems operating centre (SOC) who meet these Police requirements can monitor ATSVIVR systems.
- 1.4** A SOC must agree and sign the Police Service of Scotland and Industry approved indemnity letter and return this to the force as part of the URN acceptance procedure.
- 1.5** A URN will be issued to a SOC for the purpose of monitoring ATSVIVR systems. This URN will be issued by the Police Service of Scotland.
- 1.6** The Police response to a reported ATSVIVR system which meets the requirements set out in this appendix will be **level 1**.
- 1.7** Other types of vehicle tracking systems that operate outside of this policy will be known as type B systems and a URN will not be issued to SOC to monitor such systems.
- 1.8** Any ARC's/SOC that has existing vehicle tracking contracts (known as legacy vehicle immobilisation) with the Police may continue monitoring and reporting those existing systems. But these ARC's/SOC will not be issued with a Police Service of Scotland URN.

2. ATSVIVR REQUIREMENTS (See Annex A of Appendix)

2.1 INSPECTORATE REQUIRMENTS

For an ATSVIVR system to be accepted by an SOC the installation service shall be inspected in accordance with the provision of this document by a certification body accredited to EN 45011 by the United Kingdom Accreditation Service. The exception to this is ATSVIVR systems fitted by the Original Equipment Manufacturer (OEM) at the car manufacturing plant.

For the SOC to be acceptable to Police Service of Scotland it shall be inspected in accordance with the provisions of this document by a certification body accredited to EN 45011 with the scope of BS 5979CAT II and ISO 9001 by the United Kingdom Accreditation Service.

Appendix U continued

2.2 SYSTEM INSTALLATION REQUIREMENTS

- a. Installation shall be carried out by the car manufacturer at source, or by a dealership, or as an after market fit to the ATSVIVR manufacturers specifications.
- b. The after market fit shall only be undertaken by a company that is approved by an UKAS accredited inspectorate.
- c. The ATSVIVR system installed shall meet the installer requirements set down in the CEN TS 15213 series (*Road transport and traffic telematics – **After Theft Systems with Vehicle Immobilisation for Vehicle Recovery***).

2.3 COMMISSIONING REQUIREMENTS

- a. The commissioning of the ATSVIVR will meet the requirements laid down in the Thatcham Category 5 Criteria for After Market and OEM for System Operating Centres (SOC) monitoring after theft systems for vehicle recovery.
- b. The commissioning shall be undertaken by organisations approved by Thatcham or a UKAS accredited inspectorate.

2.4 MONITORING (SOC) REQUIREMENTS

The requirements of the SOC are:

- a. BS 5979 Category II
- b. All personnel to be vetted to BS 7858
- c. SOC parts of the CEN/TS 15213 Series
- d. CAST 14/02 – stolen vehicles
- e. BS ISO 9001:2000
- f. Category 5 criteria as listed in Appendix S

3. LEGAL REQUIREMENTS

All documentation and data pertaining to personal data of the owner of the vehicle with an AFSVIVR system installed shall be processed as per the Data Protection Act 1998.

4. POLICE ATTENDANCE

Para 4.1 of this policy does not apply to ATSVIVR – THE FOLLOWING DOES APPLY

- a. For ATSVIVR systems Police attendance will be a level 1 – Immediate/urgent.

Appendix U continued

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

5. PROCEDURES

- 5.1 When a vehicle is stolen the vehicle owner shall contact their local Police and report the incident and obtain a Crime Reference Number (CRN).
- 5.2 The vehicle owner shall then contact the SOC and report the stolen vehicle and give the SOC the CRN.
- 5.3 The SOC will then locate the stolen vehicle and contact the force.
- 5.4 The SOC will keep in touch with the force directing the Police to the location of the stolen vehicle.
- 5.5 The SOC shall keep monitoring the location of the stolen vehicle until informed otherwise by the Police.
- 5.6 If required the SOC will activate the stolen vehicle's "immobilisations" device. It is important to note that the order to activate the vehicle's immobilisation device can only be given by a Police officer who has the stolen vehicle in their line of sight.

6. MANAGEMENT INFORMATION

- 6.1 The SOC will ensure that they have a false alarm management system in place.
- 6.2 The SOC shall hold alarm statistics on all their customers and when required provide to Police Service of Scotland relevant system management statistics on request.
- 6.3 The SOC will inform customers who have repeated false alarms that they may lose Police response if the cause of the false alarm is not remedied. The SOC will keep statistics on such cases.

7. URN REQUIREMENTS

- 7.1 The SOC will apply to the Police Service of Scotland for a URN. The cost of the URN will be **£52.55 plus VAT**.

Appendix U continued

7.2 The SOC is to apply to the Chief Constable for a URN using Appendix F of this policy.

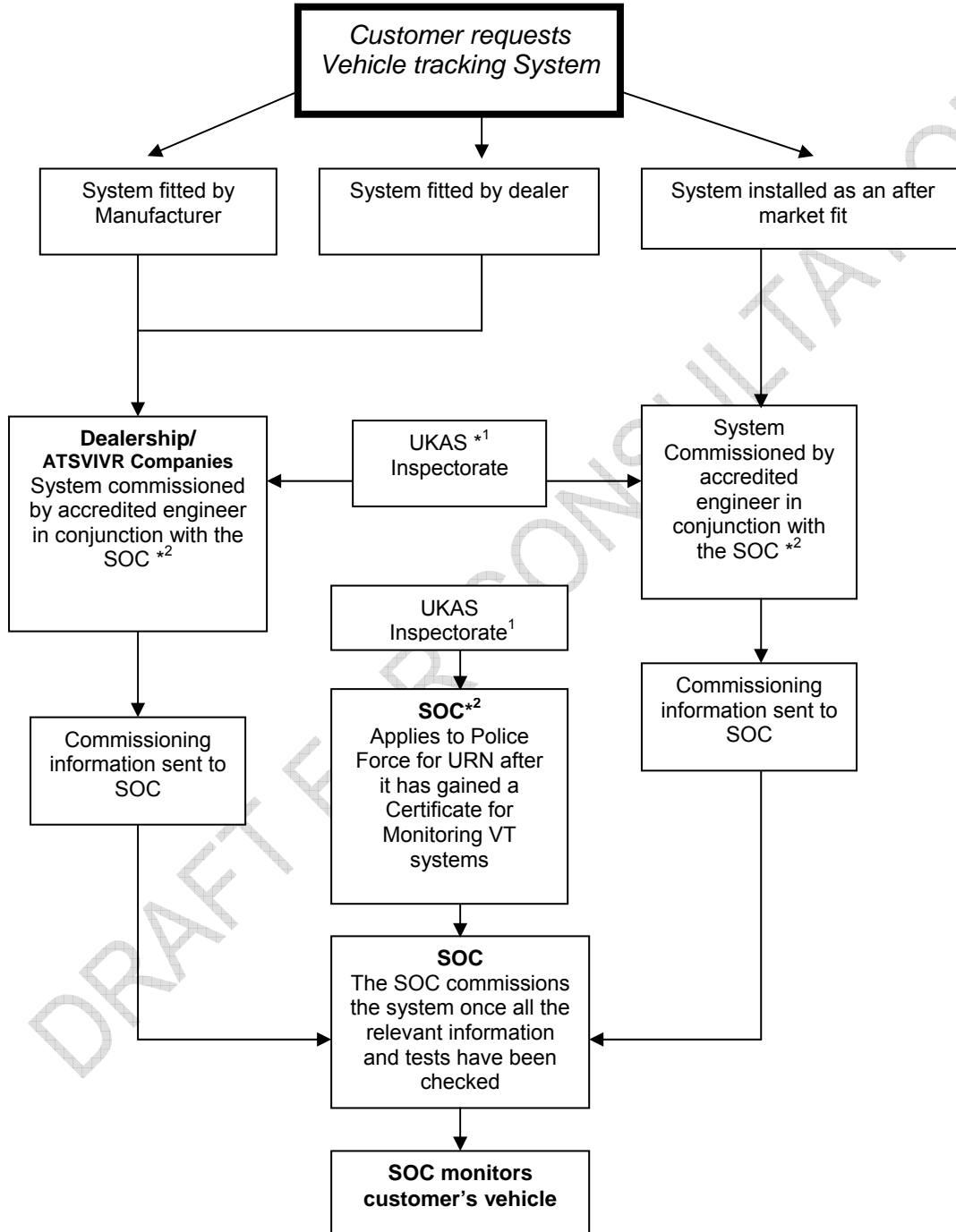
8. INDEMNITY

This document does not impose any liability on the Police Service of Scotland, its officers or the Police authority arising out of the failure or timeliness in responding to activation from an ATSVIVR system.

DRAFT FOR CONSULTATION

Appendix U annex A - Police Service of Scotland vehicle tracking requirements

Police Service of Scotland VEHICLE TRACKING REQUIREMENTS FOR THE ALLOCATION OF A URN FOR A THATCHAM CATEGORY 5 SYSTEM WITH VEHICLE IMMOBILISATION CAPABILITY



Notes:
 *1 Accredited engineer shall be vetted (BS 7858 and have a Police or CRB check).
 *2 The SOC is to submit the approved indemnity letter to Police forces.

Appendix U Annexe B - After-theft vehicle immobilisation systems indemnity

DOCUMENT FOR SYSTEM OPERATING CENTRE

To: Chief Constable, Police Service of Scotland

From

Date

Reference HOSBD 14/02 – STOLEN VEHICLE TRACKING Police Service of Scotland AND HOME OFFICE GUIDANCE TO COMPANIES ON POLICE POLICY
(including After Theft Vehicle Immobilisation Systems)

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

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

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

The SOC will not indemnify against:

- a. The failure of the vehicle immobilisation system (hardware/software) once the command has been sent.
- b. The failure of the communication network outside of the SOC control to send the signal to the target vehicle.
- c. Any failure due to faulty immobilisation system installation into the vehicle.
- d. Any delay of the activation of the immobilisation system, after the SOC has dispatched the signal, due to the geographical location of the vehicle and the time the network uses to transmit the signal from the SOC to the vehicle.

Appendix U - Annexe B continued

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

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

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

Signature _____

Name of Person _____

Job Title _____

Date _____

DRAFT FOR CONSULTATION

Appendix V - Police requirements for lone workers services

1. INTRODUCTION

- 1.1 This appendix sets out the Police requirements for the provision of lone worker services requiring Police response.
- 1.2 ARCs who meet these Police requirements will be able to apply for a URN to gain Police response for lone worker systems.
- 1.3 Alarm Receiving Centres shall have filtering and verification processes in place to reduce false alarm activations from Lone Worker Devices (LWDs) and the Police shall only be called in situations where a Police response is required. In non-threat situations other types of response from other agencies or supervisors may be required. In these circumstances the Police should not be called as this may count as a false activation.
- 1.4 The supplier shall inform the customer of the requirements of the Police Service of Scotland Security Systems Policy, including this Appendix.
- 1.5 The customer shall be trained by the supplier to use the LWD and also how to cancel any false activations that occur so as to minimise any false calls.

2 URN REQUIREMENTS

- 2.1 **The ARC will apply to the Police Service of Scotland for a URN. The cost of the URN will depend on the number of devices monitored nationally:**
- **Under 10,000 £52.55 plus VAT per annum.**
 - **10,000 – 50,000 £78.82 plus VAT per annum.**
 - **50,000 or above £105.10 plus VAT per annum.**
- All fees applicable on the anniversary of date of creation of the URN.**
- 2.2 The ARC is to apply to the Chief Constable for a URN using the Appendix F of this policy.

3 FALSE ALARMS

- 3.1 The amount of false alarms as stated in Section 4 of the main Police Service of Scotland Security Systems Policy does not apply to lone worker systems.
- 3.2 *Appendix U - Annexe B* will monitor the number of false alarms per URN and supply these numbers to the Police Service of Scotland Security Systems Group Secretariat at the end of each calendar month.

4 DEVICE REQUIREMENTS

- 4.1 Lone Worker Devices shall:
- a) Meet the lone worker device requirements laid down in BS 8484:2009

Appendix V continued

4.2 Lone Worker Suppliers shall:

- a) Meet the Lone Worker supplier requirements laid down in BS 8484
- b) Meet the requirements as laid down in Appendix S, sub clause III, except sub clause 'I'
- c) The supplier shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance the provisions of the ACPOS requirements for lone worker systems.

5. MONITORING (ARC) REQUIREMENTS

5.1 The ARC shall:

- a) Meet the ARC requirements laid down in BS 8484:2009
- b) Conform to BS 5979 Cat 11
- c) The ARC shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of the Police Service of Scotland requirements for lone worker systems.

6. LEGAL REQUIREMENTS

All the documentation and data pertaining to personal data with respect to Lone Worker Services shall be processed in accordance with the Data Protection Act 1998.

7. POLICE ATTENDANCE

7.1 Lone Worker services which meet the requirements of the Police Service of Scotland Security Systems Policy will receive a **LEVEL 1** – immediate/urgent Police response, (**see Section 4.1.1 of policy**).

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

8. PROCEDURES

8.1 When a LWD is activated the ARC shall carry out the procedures set down in BS 8484:2009 and those set down in the **response agreement** (note the response agreement does not supersede these Police Service of Scotland requirements).

8.2 The ARC operator is to determine the nature of the incident from audio information received and where safe to do so, contact the lone worker either by 2 way radio or other means to find out more about the incident to ensure the correct level of response is attained and that the Police are not called to a non emergency response.

Appendix V continued

- 8.3** Once the ARC operator has determined that the incident does require an emergency police response, the ARC operator is to contact the police giving as much information about the incident as possible including the lone worker details and any information about other responders dispatched to the incident.
- 8.4** The ARC 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 ARC operator shall monitor the incident until informed otherwise by the Police. The audio recordings of the incident may be required for Police investigation and/or evidential purposes and should be managed as per the Data Protection Act.

9. MANAGEMENT INFORMATION

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

10. INDEMNITY

This document does not impose any liability on the Police Service of Scotland, its officers or the Police authority arising out of the failure or timeliness in responding to an activation from a lone worker system, or the failure to locate the lone worker if the location information is not accurate.