Alarm Monitoring Policy- terms and conditions

Alarm Monitoring Policy- terms and conditions

INTRODUCTION

The following alarm filtering procedures adopted by Paramount SG will be used when dealing with all EXISTING and any new alarm systems.

Note: ACPOS alarm filtering requirements may differ for systems that are covered by the following police forces:

Central Scotland	**Dumfries & Galloway**	**Fife**	**Grampian**
Lothian & Borders	**Northern**	**Strathclyde**	**Tayside**

DEFINITIONS

For the purposes of this document, the following definitions have been taken from the NSI Code of Practice for Intruder Alarms Signalling to Alarm Receiving Centres (NACP14):

ALARM FILTERING	A procedure whereby remotely notified alarm conditions are intentionally delayed at the Alarm Receiving Centre and their status reviewed for the purpose of cancelling certain alarm conditions, where such cancellation is authorised by the client.
ALD	Audio Listening Device
AMD	Audio Monitoring Device
ARC	Alarm Receiving Centre
AUDIBLY CONFIRMED	Designated at the Alarm Receiving Centre by interpreting audio information received from the supervised premises and determination of a high probability that a genuine alarm has occurred.
CIE	Control and Indicating Equipment
GENUINE ALARM	Policed alarm condition which has resulted from: a) a criminal attack, damage, or attempt at such,, upon/to the supervised premises, the alarm equipment or the transmission path carrying the alarm signal; or b) actions by emergency services in the execution of their duties; or c) a call emanating from a Hold-Up alarm system made to summon urgent assistance when an assailant enters a previously defined area with the intention of harming or threatening any person within that defined area
HAS	Hold-up Alarm System
HD	Hold-up Device
HUA	Hold-up Alarm
IAS	Intruder Alarm System

Alarm Monitoring Policy- terms and conditions

MIS-OPERATION SIGNAL	Signal that is identifiable at the Alarm Receiving Centre as indicating that the intruder alarm system has mis-operated and therefore that the remotely notified alarm condition is to be cancelled and regarded as a false alert.
SEQUENTIALLY CONFIRMED	Condition emanating from two or more independent detectors, which are configured such that there is a high probability that a genuine intrusion or a genuine attempted intrusion has occurred.
SET (CLOSED)	The state of an Intruder Alarm system, or part thereof, in which an alarm condition can be sent to warning devices or receiving equipment.
UNCONFIRMED ALARM	Signal that has not been designated as audibly confirmed, visually confirmed or sequentially confirmed.
UNSET (OPEN)	The state of an Intruder Alarm system, or part thereof, in which an alarm condition cannot be sent to warning devices or receiving equipment.
VISUALLY CONFIRMED	Designation by an Alarm Receiving Centre by interpreting visual information transmitted from the supervised premises and determining that there is a high probability that a genuine alarm has occurred.
VMD	Video Monitoring Device

Alarm Monitoring Policy- terms and conditions

1. ALARM RESPONSE TIMES

Unless otherwise agreed in writing, action will be taken to establish communications with the control room of an appropriate emergency service, or to commence a filtering procedure, within the following times of receipt of the alarm signal:

a) For Fire alarms: 60 seconds for 10% of signals received (LPS1020)*
b) For Fire alarms: 30 seconds for 90% of signals received (BS5979)*
c) For Hold-up Alarms: 30 seconds for 80% of signals received and 60 seconds for 98.5% of signals received (BS5979)*
d) For other alarms: 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received (BS5979)
e) For CCTV images: 90 seconds for 80% of initial activations received and 180 seconds for 98.5% of initial activations received (BS8418)

Alarm signals/conditions to which alarm filtering is required to be applied will be subject to an intentional delay of 90 seconds before being extended to the police, as an opportunity for the alarm to be designated as a false alert and therefore cancelled as part of the alarm filtering routine.

BS8243

Criteria for sequentially confirmed intruder alarm systems:

For an alarm condition to be regarded as sequentially confirmed:

a) the IAS should be configured so that at least two separate alarm conditions are reported, each originating from an independent detector within the confirmation time;

b) the two detectors should either be of:
1) different technologies which are permitted to have overlapping areas of coverage or
2) the same single technology and not have overlapping areas of coverage.

To be regarded as independent, each detector should be configured to report alarm conditions separately to the CIE. In addition, the input signal of one detector should not influence the output of another detector.
The intruder confirmation time should be not less than 30 minutes and not more than 60 minutes.

Types of alarm condition permitted to contribute to a sequentially confirmed intruder alarm

a) Intruder
b) Intruder during entry time (detector not part of entry route)
c) Expiry of entry time
d) Tamper (not from the activated detector)

* No filtering is applied to Fire or Personal Attack alarms. If filtering is required please confirm in writing for each system it is required for

Alarm Monitoring Policy- terms and conditions

Designation of IAS signals for sequential confirmation:

1. An alarm condition from the first IAS detector to activate should initiate transmission of an unconfirmed intruder alarm to the ARC. If an independent IAS detector subsequently activates within the confirmation time, then an unambiguous sequentially confirmed intruder alarm should be presented to the ARC operator. If a separate(i.e. independently reporting) IAS detector does not activate within the confirmation time, then the IAS should be reinstated automatically.
2. Unconfirmed alarms are subject to an intentional delay of 120 seconds so that there is an opportunity for the alarm signal to be designated as being a false alert and therefore cancelled as part of the alarm filtering routine. If, during the 120 seconds, we receive a signal that is identifiable as either:
   a) being a mis-operation signal; OR
   b) indicating that the alarm system is unset
   then, in the absence of any contrary indications, the signalled alarm condition will be designated as being a false alert and regard the signalled alarm condition as cancelled (SEE POINT 12 FOR FURTHER DETAILS).
3. If a sequentially confirmed alarm is received during this time, then the alarm call will be delayed until the end of the 120 seconds, as an opportunity for the sequentially confirmed alarm to be designated as being a false alert. An exception to the delay may be made where all the following four conditions are satisfied:
   a) it has been agreed with the Client in advance to provide monitoring of setting and unsetting;
   b) the sequentially confirmed alarm is received at least 30 min after the latest time agreed for setting;
   c) the sequentially confirmed alarm is received at least 30 min before the earliest time agreed for unsetting;
   d) there is separate evidence indicating that the intruder alarm system at the supervised premises is in the “set” condition and has been in the “set” condition for at least 15 minutes.

   Note 1: Alarm filtering will not be applied to an alarm that has been preceded by a transmission fault signal from the same supervised premises during the same set period up to a maximum of 96 hours before the alarm was received.

   Note 2: Alarm filtering of an unconfirmed alarm will not continue if we receive a transmission fault signal from the same supervised premises during the set period of up to a maximum of 96 hours after the alarm has been received.
4. If a second independent detector does not activate within the confirmation time and the confirmation time expires (i.e. during the set period), the Intruder Alarm System should be reinstated so that again if one detector activates, an unconfirmed alarm occurs and the confirmation time starts. (If the Intruder Alarm System is unset before expiry of the confirmation time, then reinstatement does not need to occur).
5. At the time of re-instatement of the Intruder Alarm System, an alarm condition should not occur. To achieve this the detector(s) remaining in alarm condition at the expiry of the confirmation time should be inhibited and a ‘Zone Omit’ signal sent to the ARC to indicate that the detector(s) has (have) been inhibited. Paramount SG will inform a keyholder that detector(s) in the Intruder Alarm System are inhibited.
6. The process of reinstatement should not remove an alarm condition, so when the Intruder Alarm System is unset there should be an indication at the Control and Indicating Equipment that an alarm condition has occurred and that a restore is required.
7. Where CONFIRMATION technology is employed, it is our belief that the end-user will be best served by allowing the Central Station to filter out UNCONFIRMED alarms.
   Paramount SG sees no point in the subscriber going to the expense of installing confirmation technology, and then allowing UNCONFIRMED alarms to be passed to the police. Any possible advantage of confirmation technology will be wiped out if the subscriber's alarm is 'blacked' by the police for false alarms! **Therefore, where CONFIRMATION technology is employed, EMCS policy is that we will not police unconfirmed alarms unless instructed to do so.**

Alarm Monitoring Policy- terms and conditions

Hold-up Alarm Systems (HAS)

HASs should incorporate one or a combination of the following alarm confirmation technologies if police response has been lost and needs to be re-instated:

1) audio confirmation;
2) visual confirmation;
3) sequential confirmation;
4) telephone confirmation (call back).

An explanation of the selected combinations should be provided to the user/client to ensure the most appropriate confirmation technology is used.

Unless agreed with the client in writing, sequential confirmation should be used only in conjunction with telephone confirmation.

The installer should obtain written confirmation of the client/user's acceptance of the chosen option, and detail how the confirmation works.

Types of alarm condition permitted to contribute to a sequentially confirmed hold-up alarm

a) Hold-up
b) Tamper (not from the activated HD)

The combination of a tamper alarm condition and a HUA condition should be interpreted as a confirmed HUA.

Criteria for sequentially confirmed hold-up alarm systems:

For an alarm condition to be regarded as sequentially confirmed:

a) the HAS should be configured so that at least two separate alarm conditions are reported within the confirmation time; and

b) signals emanating from HDs should be from either;
1) two or more HDs separately identifiable at the CIE; or
2) a multi action HD.

The hold-up confirmation time should be not less than 8 hours and not more than 20 hours.

Designation of hold-up alarm (HUA) signals for sequential confirmation

1. The first HUA signal from any HD to the CIE should initiate transmission of an unconfirmed HUA to the ARC. If the CIE receives a second HUA signal from a different HD or a second signal from a multi action HD within the confirmation time, then an unambiguous sequentially confirmed HUA should be presented to the ARC operator.
2. If a HD is triggered, an unconfirmed alarm should occur and the confirmation time should start.
3. If a sequential HUA does not occur within the confirmation time, the HAS should be reinstated so that if a HD is triggered, an unconfirmed alarm occurs and the confirmation time starts.
   NOTE If the HAS is restored before expiry of the confirmation time, then reinstatement does not need to occur.

Telephone confirmation of hold-up alarm (HUA)

For systems requiring **intervention** for HUA's after loss of response we will use the following procedure: Ring site first for 20 seconds. If engaged or no answer inform police OR if password not quoted or duress code given inform police immediately.

2. CUSTOMER CANCELLATION

FIRE ALARMS: If a Customer wishes to cancel a Fire Alarm a valid password must be quoted. If the customer gives us the password but does not know whether it is a false alarm or not, the customer will be informed that the alarm will be logged as a false alarm and no further action will be taken. They will also be informed that if they subsequently find a fire on site they will have to dial 999 to inform the brigade.

OTHER ALARMS: If a Customer wishes to cancel an alarm (i.e. P/A, Intruder, Line Fault etc.) manually, we will only class it as a false alarm if the following two things occur:

1. Customer must give password AND
2. Customer must confirm to us that the alarm is a false alarm.

If the Customer gives us the password but does not know whether it is a false alarm or not, then the alarm will not be cancelled. Further action will be taken as follows:

1. We will ask the Customer if they require Police or keyholder attendance depending on the type of alarm received.
2. If the Customer is unsure we will inform them that we are going to call the police or keyholder depending on the type of alarm received.
3. If no URN or URN withdrawn we will inform a keyholder.

NB:

- For unconfirmed alarms received from residential sites we will always ring the premises first 24 hours a day, regardless of status (unless otherwise instructed).
- For confirmed alarms with status UNKNOWN we will always ring the premises first between 08:00-20:00, (unless otherwise instructed).

3. CALLING THE FIRE BRIGADE/POLICE

Paramount SG shall attempt to inform by telephone, within a reasonable time, the Appropriate Authority of any Signalled Alarm Conditions in accordance with BS5979 or LPS1020

The following procedure will be adopted when passing alarm calls to the Fire Brigade/Police:

1) Identify that it is Paramount SG calling
2) Identify the incident as:
   a) Fire
   b) Intruder
   c) Personal Attack
   d) Duress
   e) Confirmed Intruder by audio/visual/sequential
   f) Sensor Activated CCTV
   g) Line Fault
3) Supply Unique Reference Number
4) Identify the premises
5) Confirm that we will contact keyholders
6) Ask for and record the incident reference

NOTES:

1. For all Alarms if information is received from the occupier/keyholder of the protected premises that the alarm is a false alarm (and the correct password is quoted), then a second call to the police/fire brigade will be made informing them that the alarm is now cancelled, and that police/fire brigade attendance is therefore not now required. However, this does not guarantee that the fire brigade or police will cancel their response.
2. If an alarm e.g. Fire, P/A, confirmed alarm, line fault etc. has been passed to the Fire Brigade or Police, and the same alarm is received again within 30 minutes, we will not inform the Fire Brigade or Police again. In situations such as this we will ring the site and or keyholders only.
3. Police will not be informed if the URN is on level 3 or has been withdrawn.

4. KEYHOLDER CONTACT PROCEDURE

1. Following an alarm activation we will attempt to inform one contact from a list provided to Paramount SG in writing by the Customer of any Signalled Alarm Conditions in accordance with BS5979.
2. We will attempt to contact the first keyholder listed on the alarm screen, for a period of 1-minute using the primary number listed on the alarm screen.
3. Where a number is found to be *Engaged* or there is *No Reply* from that keyholder on the primary number, we will attempt any other numbers listed on the alarm screen for the keyholder.
4. The duration of each attempt shall be 1-minute. All actions will be entered onto the alarm screen log.
5. Once it is established that there is *No Reply* or that the keyholder is out we will move to the next keyholder and repeat the above, either until contact is made, or it is deemed that all numbers have been tried and there is no keyholder available.
6. After all attempts to contact keyholders have failed we will inform the appropriate police force/fire brigade that *No Keyholders are Available*. The keyholders will then be re-tried at 15 minutes intervals for the first half hour and then again after 30 minutes, and then once every hour up to a maximum of 4 hours after the alarm event.
7. For response withdrawn or keyholder only systems, we will follow the above steps 1-5 as applicable. Once it is deemed that *No Keyholders are Available* at that time we will *Sleep* the alarm for 15 minutes. The keyholders will then be re-tried at 15 minutes intervals for the first half hour and then again after 30 minutes, and then once every hour up to a maximum of 4 hours after the alarm event. Once 4-hours have elapsed without contact we will cancel the alarm with the comments *No Further Action Possible*.
8. Where the keyholder being informed is a guarding or key-holding company, we will request a reference number once the company has been informed; where this is not available the initials of the person receiving the call will be taken.
9. EMCS shall ensure that the keyholder is informed personally, a message left with a relative (especially a child) shall not be classed as *"*keyholder informed*"*.
10. Unless specifically requested in site special actions, Paramount SG shall not leave a message on keyholder answer machines. Any message that is left on an answer machine shall not be classed as "keyholder informed".
11. When contacting a keyholder, if the keyholder wishes to discuss details of system activations, resets, police response etc. we must ask for the system password first.
12. The keyholder must be informed of the exact type of alarm received, particularly whether the alarm is unconfirmed or confirmed.
13. Keyholders must be available 24 hours every day and be contactable by telephone. Answering machines or message services are not acceptable.
14. Keyholders must have their own transport and be able to attend site within 20 minutes of the initial call.
15. Keyholders must have access to appropriate codes and be conversant with the Customer's alarm equipment.

5. MONITORING OF SETTING AND UNSETTING

- Where monitoring of setting and unsetting of an Intruder Alarm System is carried out, the police will not be called to respond in relation to user deviation from the agreed time schedules for setting and unsetting. Paramount SG will contact the Customer and/or other users/keyholders as agreed with the Customer.
- Where monitoring of setting and un-setting of an alarm is carried out, you will receive daily Activation Reports. It is your responsibility to review these reports to detect any pattern of premature un-setting and contact your Customer to either agree the un-setting time is complied with or the revised times agreed and passed to Paramount SG in writing.

- Our tolerance on un-setting times is 30-seconds from the agreed un-setting time.
- Where specifically requested in writing to do so by the Customer, such request having been acknowledged and accepted by Paramount SG in writing, Paramount SG shall contact the premises and/or one contact in the event of a monitored setting/un-setting signal outside of the agreed time frame.

6. TESTS

Please note that all systems are placed on test till 18:00 hrs (unless otherwise instructed by the caller), and will automatically be taken off test at this time by the computer system. For sites that are placed on test after 18:00 hrs the caller will be asked to specify the duration of the test i.e. 1hr, 2hr etc.

Systems may only be placed on test for a maximum of 24 hours for all requests made by telephone. If a longer test period is required the request must be confirmed in writing.

NB: Alarm Engineers may place a site on test up to a maximum period of 7 days (provided a valid engineer code is quoted).

7. ENVIRONMENTAL ALARMS

Examples of these types of alarms are temperature, boiler, lift etc. Action will be taken every time an environmental type alarm is received, however, the same keyholder contact procedure will be used as for other types of alarms.

8. BATTERY FAILURE SIGNALS

A Battery Failure signal is received when the voltage to the alarm panel has dropped substantially. This can occur when either the mains power has been off for a long period OR there is a fault.
EMCS will contact the Customer and/or keyholders, and will advise them to contact their alarm company immediately in order for the failure to be correctly diagnosed and fixed (if req'd).

9. TAMPER DETECTION

AMDs, ALDs, VMDs and imaging devices, and the circuit interconnections for these devices should be provided with tamper detection in accordance with the standard applicable to the IAS.

10. MISCELLANEOUS

- Paramount SG will carry out any reasonable special instructions provided in writing by the Customer upon receipt of Signalled Alarm Conditions provided always that Paramount SG reserves the right to disregard such special instructions if impracticable to comply with or otherwise in exceptional circumstances.

- Paramount SG will provide to the Customer in writing periodic reports detailing Signalled Alarm Conditions, and false alarms and data regarding errors or faults in the End User equipment and Customer equipment, to enable the Customer to identify and remedy such errors or faults.

- Paramount SG shall, where specifically requested in writing to do so by the Customer such request having been acknowledged and accepted by Paramount SG in writing; inform the Customer by telephone of any Signalled Alarm Conditions not covered by BS5979.

- Paramount SG shall provide to the Customer remote access to RSD to enable the Customer to review

Signalled Alarm Conditions, false alarms and other data relating to the Customer, or where the Customer has an End User to the End User, in accordance with the Agreement.

11. ALARM FILTERING PROCEDURE

FIRE ALARM:
(premises open)
Call premises first at all times (maximum of 60 seconds) - if engaged or no answer Fire Brigade informed.

NB - Keyholders will not be informed if the premises are open, **unless** specifically asked to do so in writing **or** if advised by brigade of non-attendance until confirmed.

(premises unknown)
08:00-20:00 call premises first (maximum of 60 seconds) - if engaged or no answer Fire Brigade and keyholders informed.

(premises closed)
Fire Brigade informed.
Keyholders informed

NB – If site or keyholders request the Fire Brigade at any time during the activation or immediately after the activation, we will notify the brigade immediately.

HOLD UP ALARM:
Police informed
NB – If status is closed when the HUA activation is received we will also notify keyholders.

For systems where confirmation of HUA signals is being utilised we will use the following procedure:

Telephone Confirmation - Ring site first for 20 seconds. If engaged or no answer inform police OR if password not quoted or duress code given inform police immediately.

Designation of hold-up alarm (HUA) signals for sequential confirmation:

UNCONFIRMED HUA:
Keyholders informed (if no reply from premises / False Alarm Code not known)

CONFIRMED HUA:
Police informed

Note - The combination of a tamper alarm condition and a HUA condition should be interpreted as a confirmed HUA (see section 1 – BS8243 - Types of alarm condition permitted to contribute to a sequentially confirmed HUA).

DESIGNATION OF IAS SIGNALS FOR SEQUENTIAL CONFIRMATION

UNCONFIRMED ALARM:
(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

Alarm Monitoring Policy- terms and conditions

UNCONFIRMED ALARM (See note below for unconfirmed alarms installed before Oct 2001):
(premises closed)
Keyholders informed

SEQUENTIALLY CONFIRMED ALARM:
(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

SEQUENTIALLY CONFIRMED ALARM:
(premises closed)
Police & Keyholders informed

Note - The combination of a tamper alarm condition and an intruder alarm condition should be interpreted as a confirmed alarm (see section 1 – BS8243 - Types of alarm condition permitted to contribute to a sequentially confirmed intruder alarm)

NB - SYSTEMS INSTALLED BEFORE OCTOBER 2001:

UNCONFIRMED ALARM:
(premises closed)
Police & Keyholders informed

12. MIS-OPERATION SIGNAL

All Intruder and Hold-up Alarm Systems should either:

a) Send Open/Close signals to indicate status of protected premises. **UNCONFIRMED** intruder alarms received from premises that utilise Open/Close signalling, and indicate **closed,** will automatically be delayed for **120 seconds** to await receipt of an **OPEN** signal. If a sequentially confirmed alarm is received during this time, then the alarm call will be delayed until the end of the 120 seconds, as an opportunity for the sequentially confirmed alarm to be designated as being a false alert

OR

b) Generate a secondary signal (either on a separate channel or a restore from the same channel) following alarm activation to indicate mis-operation of the alarm system. This practice is commonly referred to within the industry as Alarm and Abort.

The means to conform to at least one of these options should be present whenever there is a possibility of an alarm signal being transmitted to the ARC.

OPEN AS ABORT:

Sites that transmit an intruder type event e.g. intruder alarm, confirmed alarm, followed by an OPEN signal within **120 seconds** will AUTOMATICALLY be screened out by our computer system with NO ACTION TAKEN.
Sites that transmit an **UNCONFIRMED INTRUDER** alarm followed by an OPEN signal AFTER **120 seconds** will be CANCELLED manually by one of our operators with NO FURTHER ACTION TAKEN (SEE NOTE BELOW).

ALARM & ABORT SIGNAL:

Sites that transmit an intruder type event e.g. intruder alarm, confirmed alarm, followed by an ABORT signal within **120 seconds** will AUTOMATICALLY be screened out by our computer system with NO ACTION TAKEN.

Sites that transmit an UNCONFIRMED INTRUDER alarm followed by an ABORT signal AFTER **120 seconds** will be CANCELLED manually by one of our operators with NO FURTHER ACTION TAKEN (SEE NOTE BELOW).

Installers, who wish to use the Alarm & Abort method, should transmit the secondary signal (ABORT) on channels 4-8.UNDER NO CIRCUMSTANCES WILL AN ABORT SIGNAL BE ACCEPTED ON CHANNELS 1-3. The channel to be used must be specified on the Request for Connection Form.

Paramount SG can also abort INTRUDER alarms that are followed by a RESTORE signal (please notify us in writing if you wish us to set this up). All chips programmed by EMCS will automatically have RESTORE signals programmed as standard for all alarm channels. Chips or programmable panels programmed by an alarm company engineer MUST have RESTORE signals programmed in.

13. ALARMS FROM PREMISES STATUS UNKNOWN

INTRUDER alarms from systems that are not currently transmitting a **mis-operation** signal will be classed as alarms from PREMISES WITH STATUS UNKNOWN.

On receipt of INTRUDER alarms where the premises status is unknown, they will be actioned as follows:

UNCONFIRMED ALARM:
Residential: Premises contacted 24 hours a day.
Commercial: 08:00-20:00 Premises contacted 1st
Keyholders informed (if no reply from premises / False Alarm Code not known)

SEQUENTIALLY CONFIRMED ALARM:
Residential: Premises contacted 24 hours a day.
Commercial: 08:00-20:00 Premises contacted 1st
Police & Keyholders informed (if no reply from premises / False Alarm Code not known)

14. REDCARE LINE FAULT SIGNALS

To be able to fully monitor the REDCARE Line Fault Signals, EMCS requires that **ALL** REDCARE systems transmit Open / Close signals. Accordingly, **ALL** chips supplied by EMCS will have Open / Close programmed as standard.

Line Fault signals received from REDCARE systems will not be passed to the Police.

Redcare Line Fault with Premises OPEN:
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

Redcare Line Fault with Premises CLOSED:
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

Redcare Line Fault Premises STATUS UNKNOWN:
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

Any **LINK DOWN** and **LINK UP** (REDCARE NETWORK NO RESPONSE) messages will be passed to site/keyholders ONLY.

15. SIGNALS FROM DUAL SIGNALLING SYSTEMS

This section deals with signals from dual signalling systems e.g. REDCARE products, DUALCOM products, EMIZON etc.

There are two circumstances in Intruder Alarm Systems installed in accordance with BS 8243 where there might be high confidence that there is genuine intrusion or genuine attempted intrusion, therefore requiring a police response:

a) If a transmission fault signal is received followed by an alarm signal, or vice versa, from the same supervised premises during a single set period of up to a maximum of 96 hours.
b) If two transmission fault signals exist at the same time from the supervised premises, one from each of two transmission paths of different technologies (e.g. cable and radio) during a single set period of up to a maximum of 96 hours.

The combination of a transmission fault signal and a HUA condition should be interpreted as a confirmed HUA.

UNCONFIRMED ALARM:
(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

UNCONFIRMED ALARM:
(premises closed)
Keyholders informed (if no reply from premises / False Alarm Code not known)

UNCONFIRMED ALARM:
(premises status unknown)
Keyholders informed (if no reply from premises / False Alarm Code not known)

CONFIRMED ALARM: (i.e. Intruder Alarm followed or proceeded by a Line Fault or Radio Signal Fail during a single set period of up to a maximum of 96 hours – see notes on page6)
(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

CONFIRMED ALARM: (i.e. Intruder Alarm followed or proceeded by a Line Fault or Radio Signal Fail during a single set period of up to a maximum of 96 hours – see notes on page6)
(premises closed/unknown – for unknown same procedure as section 11 will be followed)
Police & Keyholders informed

LINE FAULT & RADIO POLL FAIL: (i.e. Exist at same time during a single set period of up to a maximum of 96 hours)
(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

Alarm Monitoring Policy- terms and conditions

LINE FAULT & RADIO POLL FAIL: (i.e. Exist at same time during a single set period of up to a maximum of 96 hours)
(premises closed/unknown – for unknown same procedure as section 11 will be followed)
Police & Keyholders informed

LINE FAULT:
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

GSM FAIL/GPRS FAIL (Dualcom Systems):
Log Only

GSM FAIL (Redcare Systems):
Log only provided that poll is successful on landline. If land line not responding i.e., in fault then:

(premises open)
Keyholders informed (if no reply from premises / False Alarm Code not known)

(premises closed/unknown – for unknown same procedure as section 11 will be followed)
Police & Keyholders informed

Redcare Secure using PSTN

- 955 alarm is line fault (PSTN voltage fail) – Key Holder Response
- 1022 alarm is radio fault (Polling of wireless has failed – server generated) – Key Holder Response
- 1023 alarm is also line fault (Polling of line has failed – server generated) – Key Holder Response
- 955 followed by a 1022 is both paths gone (confirmed alarm) – Police Response
- 1022 followed by a 1023 is both paths gone (confirmed alarm) – Police Response
- 1023 followed by a 1022 is both paths gone (confirmed alarm) – Police Response
- 955 followed by Intruder – Police Response
- 1022 followed by intruder (confirmed alarm) – Police Response
- 1023 followed by intruder (confirmed alarm) – Police Response

Dualcom GPRS using PSTN

- GPRS fail is radio fault – Log only
- Line fault is line down – Key Holder Response
- Polling fail is both paths down – Key Holder Response
- GPRS fail followed by Poll fail – Log only
- Line fault followed by Poll fail – Key Holder Response
- GPRS fail followed by Intruder (confirmed alarm) – Police Response
- Line fault followed by Intruder (confirmed alarm) – Police Response

16. AUDIBLY CONFIRMED ALARM SIGNALS

Paramount SG currently offers facilities for the monitoring of the following types of Audio Confirmation equipment (which are all initiated by Paramount SG (i.e. dial back):

AV 60	-	Available from ICM Developments
TalkDac		-Available from DA Systems
Verified Audio	-	Available from Verified Systems
CSL Audio	-	Available from CSL Systems

Installers must specify the type of equipment used when completing a Request for Central Station Connection form.

In the case of audio confirmation of intruder detection, the listen-in periods will be a minimum of 60 seconds and include all of the stored audio if live audio does not provide sounds consistent with intrusion or attempted intrusion into the supervised premises. Therefore, there should be:

i. stored audio of not less than 10 seconds immediately before an alarm condition, which is stored at the supervised premises ready for transmission to the Alarm Receiving Centre.
ii. stored audio of not less than 15 seconds immediately after an alarm condition, which is stored at the supervised premises ready for transmission to the Alarm Receiving Centre

As soon as Paramount SG reaches a decision that the sounds emanating from the supervised premises are consistent with intrusion or attempted intrusion into the supervises premises, the alarm signal will be designated as being an audibly confirmed alarm signal.

If sounds are inconclusive with regard to intrusion or attempted intrusion into the supervised premises, the alarm signal will be designated as an unconfirmed alarm (unless a sequentially confirmed alarm occurs).

UNCONFIRMED ALARM:
(premises open)
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

AUDIBLY CONFIRMED ALARM (UNLESS WRITTEN AUTHORISATION "TO CALL POLICE' IS GIVEN):
(premises open)
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

Alarm Monitoring Policy- terms and conditions

UNCONFIRMED ALARM:
(premises closed)
Keyholders informed

AUDIBLY CONFIRMED ALARM:
(premises closed)
Police & Keyholders informed

UNCONFIRMED ALARM:
(premises unknown)
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

AUDIBLY CONFIRMED ALARM:
(premises unknown)
Police & Keyholders informed

RESPONSE
Paramount SG cannot guarantee the response of third parties. Police, Fire, or security guarding companies will be contacted in accordance with instructions provided by our customers. We cannot guarantee that any third party will attend your premises.

17. VISUALLY CONFIRMED ALARM SIGNALS

Installers must specify the type of equipment used when completing a Request for Central Station Connection form. Also, a detailed list is required of where the cameras are installed within the protected premises. Intruder alarm systems equipped with visual confirmation of intruder detection should also be configured to generate sequentially confirmed alarms.

Imaging devices should be sited to avoid light sources that could interfere with viewing by our operator and the field of view should be illuminated so that we receive a clear image. The imaging device should also view all of the area of coverage of any accompanying detector. After an alarm condition there should be a minimum of three images transmitted to the Alarm Receiving Centre, one image at the time of the alarm condition or the video monitoring device (VMD) activation, and two more images afterwards within 5 seconds of the alarm condition or the VMD activation.

As soon as Paramount SG reaches a decision that the images emanating from the supervised premises are consistent with intrusion or attempted intrusion at the supervises premises, the alarm signal will be designated as being a visually confirmed alarm signal.

If images are inconclusive with regard to intrusion or attempted intrusion into the supervised premises, the alarm signal will be designated as an unconfirmed alarm (unless a sequentially confirmed alarm occurs).

UNCONFIRMED ALARM:
(premises open)
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

VISUALLY CONFIRMED ALARM (UNLESS WRITTEN AUTHORISATION "NOT TO CALL POLICE" IS GIVEN):
(premises open)
Police & Keyholders informed

UNCONFIRMED ALARM:
(premises closed)
Keyholders informed

VISUALLY CONFIRMED ALARM:
(premises closed)

Police & Keyholders informed

UNCONFIRMED ALARM:
(premises unknown)
Premises informed
Keyholders informed (if no reply from premises / False Alarm Code not known)

VISUALLY CONFIRMED ALARM:
(premises unknown)
Police & Keyholders informed

18. CCTV ACTIVATIONS for the purpose of verification of activation from IDS. (Internal systems)

For BS8418 systems the Customer and not the installer must send this information with an Inventory of CCTV equipment installed for the purposes of verification of IDS systems.
Video verified internal IDS

NB – Any system requiring police response must have a URN and conform to BSEN50131 - Code of practice. The response below will be taken in conjunction with the Response Plan for each site supplied by the Customer.

1. View and study the captured alarm frame(s) for signs of activity. Once these frames have been viewed re-read the site special instruction listed on the screen and follow instructions.
2. Having viewed the alarm frame(s) accept any further alarms from the site.
3. View live images from the verification camera that was activated for a minimum of 10 seconds.
4. Proceed to multi-view and view images from all other verification cameras.
5. If there is no cause for the alarm visible, enter the comments “Nothing Suspicious Seen” on the alarm screen, clear down the alarm activation and clear down the receiver. This step shall only be taken if there are no special instructions requiring other actions, i.e. to inform keyholder upon activation.
6. If activity of any kind is seen this must be noted on the Alarm Screen (animal activity, wind-blown rubbish etc.).
7. If persons or suspicious activity is observed, the audio system shall be used and a keyholder will be informed.
8. If an attempt to break-in to the premises is being made, or an actual break-in is in progress pass the event to either the relevant police force (if there is a URN) and/or a keyholder giving full details of all events seen.

9. Stay on-line to the site if requested by Police to enable updates to be passed to the police officers responding. Full details of any activity shall be logged on the Alarm Screen. Before police action is taken double-check the site special instructions to ensure police action is required.

10. When issuing audio follow any instructions pertaining to the text of such an audio message. Once the alarm has been passed to the police pass any other information to the police if further incidents are observed on the receivers.

11. Ensure all incidents are logged with details of cause of activation and action taken.

12. If privacy zones are viewed, this must be logged, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the contractual patrol (this applies for any incident or routine camera patrol).

19. REMOTE RESETTING OF SIGNALLING SYSTEMS

INTRODUCTION

It is the policy of Paramount Sg when carrying out the Remote Resetting of Signalling Systems, to at **ALL** times follow the procedures and guidelines laid down in:

BS 8473:2006 - Intruder and hold-up alarm systems – Management of false alarms

PD 662:2004 – Scheme for the application of European Standards for intruder and hold-up alarm systems

prEN 50131-1:2004 – Alarm Systems – Intrusion Systems – Part 1: System Requirements

BS 4737-4-4.2: 1986 - Intruder alarm systems in buildings – Part 4: Codes of Practice – Section 4.2: Code of practice for maintenance and records

The procedure stated below has been implemented with immediate effect.

SCOPE

Resets Given to Subscribers

The Remote Resetting of Signalling Systems will ONLY be authorised by Paramount SG personnel if the cause of the alarm activation is determined by Central Station Staff in conjunction with the user or alarm company service technician, to fall into one of the following categories:

1. **COMPANY-RELATED FALSE ALARMS** –
   NOTE – Incorrect siting, coverage, range or choice of detector would fall under point i, ii and iii below.

   i. **System Design** – Any false alarm attributable to incorrect design of the alarm installation or the faulty application of detection devices; includes any false alarm attributable to electrical interference or transients from which the I&HAS (Intruder & Hold-up Alarm Systems) should be immune, such as mains transients,

effects of electrical storm, CB or radio interference; also includes the effects of mains power failure and activations caused by rodents, insects, birds, bats, etc.

ii. **System Installation** – Any false alarm attributable to poor workmanship (except as covered by iii below)

iii. **System Maintenance/Repair** – Any false alarm attributable to lack of preventative maintenance or to poor workmanship in carrying out repairs during breakdown calls.

iv. **Procedural Failure** – Any false alarm attributable to failure to put an I&HAS onto test when carrying out maintenance or repair.

v. **Control Equipment** – Any false alarm directly attributable to an electrical or mechanical failure of control equipment which cannot be attributable to any other category, and which would result in repair or replacement of the control equipment or any part of the control equipment.

vi. **Movement Detectors** - Any false alarm directly attributable to an electrical or mechanical failure of a movement detector, which cannot be attributed to any other category and which would result in the repair or replacement of the movement detector or of any part of the movement detector.

vii. **Other Electrical/Electronic Devices** - Any false alarm directly attributable to an electrical or mechanical failure of any electrical or electronic device, other than one listed above, which cannot be attributed to any other category, and which would result in the report or replacement of the electrical or electronic device or of any part thereof.

viii. **Non-Electrical/Electronic Device** - Any false alarm directly attributable to an electrical or mechanical failure but which cannot be attributed to any other category and which would result in the repair or replacement of the failed item.

2. **OPERATOR-RELATED FALSE ALARMS** –

i. **Insecure Premises** - any false alarm attributable to the condition of doors, windows and other openings into the supervised premises.
NOTE - openings might or might not be supervised by I&HAS detectors but are sited within the I&HAS supervised area.

ii. **Operator Error** - any false alarm attributable to actions by untrained or inadequately trained operators of the I&HAS.

iii. **Wrong Entry Procedure** - any false alarm attributable to action by the operator, which differs from the operational instructions given to the client on the correct course of actions to follow when entering the supervised premises.

iv. **Wrong Exit Procedure** - any false alarm attributable to any deviation by the operator from the operational instructions given to the client on the correct course of action to follow when leaving the supervised premises.

v. **Twenty-Four Hour Equipment** - any false alarm attributable to the deliberate or accidental operation of continuously (twenty-four hour) operated detectors/devices on the I&HAS.

vi. **Irregular Opening / Closing** – any false alarm attributable to the opening/closing of premises outside of the periods agreed with the installing/maintaining alarm company.
NOTE – For systems installed in accordance with DD 243 the police would not be notified of irregular opening or closing of the premises outside the agreed time schedules.

Alarm Monitoring Policy- terms and conditions

3. **ARC-RELATED FALSE ALARMS** –

Examples of ARC related false alarms include the following:

- Human error
- Policing a system while system is on test
- Failing to put systems on test
- Policing unconfirmed alarms from confirmed systems
- Passing of incorrect information to police
- ARC equipment failure

NOTE:
The Remote Reset procedure listed below will only apply to policed activations. Where an alarm system has not been passed to the police the Customer will be allowed 6 remote resets in 28 days. However, remote resets will not be issued if points 1, 2 or 3 apply. Also, if no alarm signal of any kind is received (e.g. P/A, Intruder, Confirmed alarm, Line Fault, Set Fail, Technical fault) a remote reset will not be issued except to an alarm company engineer.

For policed activations Remote Resets will NOT be given to a subscriber under ANY circumstances where:

1. identification of the operator and the protected premises is not possible from the Password given by the telephone caller.

2. cause of alarm is not known – the cause of the remotely notified alarm condition has not been clearly described by the subscriber, or the description given is not consistent with the remotely notified alarm condition having been caused by operator error.

3. there is faulty equipment – the description of the cause of the remotely notified alarm condition given by the subscriber is consistent with there being no requirement for a corrective maintenance visit.

4. more than **2**-policed alarm conditions have occurred in the last 12 months.

NOTE: A remote reset will be permitted if a genuine alarm, or genuine confirmed alarm, has occurred. However, Paramount SG will advise the operator that insurance cover could be invalidated if a service technician's visit does not take place and the I&HAS is subsequently found not to be in full working order.

Where reset is denied, the alarm company's service technician should visit the supervised premises for the purpose of identifying the cause of the alarm condition, carrying out corrective maintenance/action and ensuring that the I&HAS is in full working order and:

a) **in the case of a false alarm due to operator error, educating the operator in the operation of the I&HAS, and the avoidance of false alarms**
b) **if design faults are noted these are reported to the Systems Performance Manager by the next working day.**

Alarm Monitoring Policy- terms and conditions

CONTACT PROCEDURE

A customer requiring a Remote Reset must telephone the Central Station on 0870 399 0999

Remote Resets will ONLY be given to subscribers who can quote either their SITE PASSWORD or their Site ID NUMBER.

RESETS GIVEN TO ALARM COMPANY SERVICE TECHNICIANS

Central Station Staff will **ALWAYS** give a Remote Reset to alarm company service technicians who quote **EITHER** the individual ENGINEER ID CODE **OR** the SITE PASSWORD / CHIP NUMBER. Where an Engineer ID Code has been quoted, remote resets given to alarm company service technicians, will not be counted when totalling the number of resets given to determine if the maximum number of Resets has been exceeded.

FINAL DECISION

AT ALL TIMES THE FINAL DECISION WITH REGARDS TO THE GRANTING OF REMOTE RESETS WILL REST WITH THE ON-DUTY CENTRAL STATION SUPERVISOR. AT ALL TIMES THE MANAGEMENT OF EMCS WILL BACK THE JUDGEMENT OF THE SUPERVISOR IN THIS MATTER.

9. FORCE MAJEURE

Any failure by the Company to fulfil any of its obligations under the terms of this Contract due to reasons beyond its control shall not be considered a breach of this Contract.

10. APPLICABLE LAW

This Contract is governed by the laws of England and Wales, Scotland or Northern Ireland as the case may be and each party submits to the jurisdiction of the courts thereof.

11. ACCEPTANCE BY CUSTOMER

The customer undertakes and agrees to accept all of the terms and conditions stated within this document IN FULL upon once placing an order upon the company.

12. CLAIMS BY CUSTOMER

The Company has provided limited insurance cover for itself with indemnity for claims made against it in respect of accident, injury, loss or damage. Cover also extends to failure to perform and wrongful advice given unwittingly. Any such claim must be made within 60 days of the loss occurring, claims after that period will not be accepted.

13. RIGHT TO AMMEND, UPDATE OR CHANGE

The company reserves the right to amend, update or change the terms and conditions as defined above, with 30 days written notice to the customer.