Alarm Monitoring Policy

Date	Author	Summary of changes
23/05/2024	MARSTA	Revised version – annual update
27/09/2024	CARBOO	Logo Updated
23/05/2024	ROXPAL	Summary of changes added to policy
07/05/2024	ROXPAL	Revised version issued by MARSTA
25/04/2025	ROXPAL	Updated to include all updates to summary of tables
07/05/2025	MARSTA	Annual Review

Contents

INTRODUCTION 2
DEFINITIONS 2
1.GDPR 3
2.ALARM RESPONSE TIMES 3
3.BS8243 4
4.CUSTOMER CANCELLATION 7
5.CALLING THE FIRE & RESCUE SERVICE/POLICE 7
6.KEYHOLDER CONTACT PROCEDURE 8
7.MONITORING OF SETTING AND UNSETTING 9
8.TESTS 9
9.ENVIRONMENTAL ALARMS 10
10.BATTERY FAILURE SIGNALS 10
11.TAMPER DETECTION 10
12.MISCELLANEOUS 10
13.ALARM FILTERING PROCEDURE 11
14.MIS-OPERATION SIGNAL 12
15.ALARMS FROM PREMISES STATUS UNKNOWN 13
16.REDCARE LINE FAULT SIGNALS 13
17.SIGNALS FROM DUAL SIGNALLING SYSTEMS 14
18.AUDIBLY CONFIRMED ALARM SIGNALS 15
19.VISUALLY CONFIRMED ALARM SIGNALS 16
20.CCTV ACTIVATIONS 17
21.REMOTE RESETTING OF SIGNALLING SYSTEMS 18
22.CONTACT PROCEDURE 20
23.RESETS GIVEN TO ALARM COMPANY SERVICE TECHNICIANS 20
24.FINAL DECISION 20

Alarm Monitoring Policy

INTRODUCTION

The following alarm filtering procedures adopted by ARC 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 (Fire Alarm System)
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

Alarm Monitoring Policy

IAS	Intruder Alarm System
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
AAH	Auto Alarm Handler

1. GDPR

The ARC holds personal information on keyholders/system users of your system installations for the purposes of passing information to and from these individuals. This information is limited to such as the active state of the system, CCTV images (where relevant to the system being monitored) and information that may have been passed to the emergency services. This information is retained both within our control software data base and voice recordings.

Retention Periods:

- The data base is retained for the life of the contract plus 3 years
- Voice recordings are retained for a period of 3 months
- CCTV Images are retained for 31 days unless we have justification for retaining for a longer period such as for evidence in a criminal case.

ARC do not pass this information to any person or organisation outside of validated system users/keyholders, the emergency services or to you as the Installer/Maintainer.

You have a right of access to this information, it's correction if inaccurate and for its deletion as defined within our Data Protection and Privacy Policy.

2. 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*
b) For Fire alarms: 30 seconds for 90% of signals received*
c) For Hold-up Alarms: 30 seconds for 80% of signals received and 60 seconds for 98.5% of signals received*
d) For other alarms: 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received
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 120 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.

3. 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:
   a. different technologies which are permitted to have overlapping areas of coverage or
   b. 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)

Alarm Monitoring Policy

Designation of IAS signals for sequential confirmation:

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

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 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.

1. 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).

2. 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.

3. 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).

4. 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. ARC will inform a keyholder that detector(s) in the Intruder Alarm System are inhibited.

5. 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.

6. Where CONFIRMATION technology is employed, it is our belief that the Customer will be best served by allowing the ARC to filter out UNCONFIRMED alarms.

7. ARC 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, ARC policy is that we will not police unconfirmed alarms unless instructed to do so.

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:

a) audio confirmation
b) visual confirmation
c) sequential confirmation
d) telephone confirmation (call back)

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

Unless agreed with the Customer 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:

b) Signals emanating from HDs should be from either:
    a. Two or more HDs separately identifiable at the CIE; or
    b. A multi action HD

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

Alarm Monitoring Policy

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

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.

If a HD is triggered, an unconfirmed alarm should occur, and the confirmation time should start.

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)

NATIONAL POLICE CHIEFS' COUNCIL GUIDELINES – CONFIRMATION OF HOLD-UP ALARMS:

We request that you cease to use telephone call-back for confirmation of hold-up alarms in commercial premises with immediate effect in relation to all new cases involving reinstatement of police response to hold-up alarms.

The ceasing of telephone call-back for hold-up alarms in commercial premises is not retrospective. However, we recommend you should review existing premises where telephone call-back is used to ensure the arrangements are satisfactory. The objective here is to drive down the number of false hold-up alarms in as many cases as possible.

Telephone call-back for confirmation of hold-up alarms can continue to be used in domestic premises along with audio, visual and/or sequential confirmation.

For systems requiring **intervention** for HUA's after loss of response for **commercial** sites we now recommend that audio, visual and/or sequential confirmation should be used.

For systems requiring **intervention** for HUA's after loss of response we can use the following procedure for **residential/domestic** sites:

a) 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

4. CUSTOMER CANCELLATION

FIRE ALARMS: If a customer wishes to cancel a Fire Alarm, please ask them for a cause of the activation. If the customer informs us, it is a false alarm but does not know the cause of activation, 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 fire & rescue service.

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:

a) Customer must give password AND

b) Customer must confirm to us that the alarm is a false alarm and provide a cause of the activation

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

a) We will ask the Customer if they require Police or keyholder attendance depending on the type of alarm received
b) 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
c) If no URN or URN withdrawn, we will inform a keyholder

NB:

- For 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)

5. CALLING THE FIRE & RESCUE SERVICE/POLICE

ARC shall attempt to inform by telephone, within a reasonable time, the Appropriate Authority of any Signalled Alarm Conditions in accordance with EN50518.

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

a) Identify that it is ARC calling
b) 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
c) Supply Unique Reference Number
d) Identify the premises i.e. confirm full name and address
e) Confirm that we will contact keyholders
f) Ask for and record the incident reference

NOTES:

1. If we cannot contact the police after 5 minutes ring keyholders. Inform them that if they find a problem on site to ring 999. However, if the keyholder requests us to keep trying then we can try again for another 5 minutes.
2. 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 & rescue service will be made informing them that the alarm is now cancelled, and that police/Fire & rescue service attendance is therefore not now required. However, this does not guarantee that the Fire & rescue service or police will cancel their response.
3. If an alarm e.g. Fire, P/A, confirmed alarm, line fault etc. has been passed to the Fire & rescue

service or Police, and the same alarm is received again within 30 minutes, we will not inform the Fire & rescue service or Police again. In situations such as this we will ring the site and or keyholders only.

4. At this stage we may also inform the keyholder that the zone which is activating will be isolated for 60 minutes. If after 60 minutes, it is still coming through then we may ring the keyholder again and inform them it will be isolated for 24 hours. If the zone cannot be isolated for certain systems, then the category may be placed on test – but again the keyholder must be informed of this e.g. all power fail type signals have been placed on test for 24 hours.
5. Police will not be informed if the URN is on level 3 or has been withdrawn.

6. KEYHOLDER CONTACT PROCEDURE

Following an alarm activation, we will attempt to inform one contact from a list provided to ARC in writing by the Customer of any Signalled Alarm Conditions in accordance with EN50518.

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.
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.

The duration of each attempt shall be 1-minute. All actions will be entered onto the alarm screen log.

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.

After all attempts to contact keyholders have failed we will inform the appropriate police force/Fire & rescue service that No Keyholders are Available. The keyholders will then be re-tried again after 15 minutes and then after 30 minute intervals twice, up to a maximum of 1 hour and 15 minutes after the alarm event.

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 again after 15 minutes and then after 30 minute intervals twice, up to a maximum of 1 hour and 15 minutes after the alarm event. Once this time has elapsed without contact, we will cancel the alarm with the comments No Further Action Possible.

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.

ARC shall ensure that the keyholder is informed personally, a message left with a relative (especially a child) shall not be classed as “keyholder informed”.

Unless specifically requested in site special actions, ARC 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”.

When contacting a keyholder, if the keyholder wishes to discuss details of system activations, resets, police response, other keyholder information etc. we must ask for the system password first.

If the keyholder states they are on site OR that the alarm is a false alarm OR when a keyholder has the same telephone number as the site, then we will request their password before we can close the alarm down. NB - This does not apply to guarding companies who are on site.

The keyholder must be informed of the exact type of alarm received, particularly whether the alarm is unconfirmed or confirmed.

The keyholder must be informed of the full name and address including postcode of the site that has activated.

Keyholders must be available 24 hours every day and be contactable by telephone. Answering machines or message services are not acceptable.

Keyholders must have their own transport and be able to attend site within 20 minutes of the initial call.

Keyholders must have access to appropriate codes and be conversant with their alarm equipment.

For low priority alarms e.g. AC Power Fail, Battery Fail, BT Link Down, BT Link OK, Fault Alarms, Mains Failure, Low Battery, Low RF Battery, Panel Fault, Power Loss, PSTN Low Voltage and System Trouble, a single attempt will made to contact the client/clients appointed key-holders advising them of the issue after which the alarm will be cleared down with the comments No Further Action Possible.

7. 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. ARC 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 ARC 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 ARC in writing, ARC shall contact the premises and/or one contact in the event of a monitored setting/un-setting signal outside of the agreed time frame.

8. TESTS

Please note that all systems placed on test will be under the instruction of the caller they will be asked to specify the duration of the test i.e. 1hr, 2hr etc. If the caller doesn't call back to confirm they have finished testing (Or require further testing) the Test will expire via the computer system and the system will be placed back live for Monitoring

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.

Alarm Monitoring Policy

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

9. ENVIRONMENTAL ALARMS

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

10. 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.

ARC will contact the Customer and/or keyholders and will advise them of the activation received, The ARC will then offer the Customer and/or keyholders if they require an Alarm Technician (if req'd).

11. 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.

12. MISCELLANEOUS

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

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

ARC shall, where specifically requested in writing to do so by the Customer such request having been acknowledged and accepted by ARC in writing; inform the Customer by telephone of any Signalled Alarm Conditions not covered by BS EN 50518.

ARC shall provide to the Customer remote access to the customer portal to enable the Customer to place their fire alarms on test and 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.

Alarm Monitoring Policy

13. ALARM FILTERING PROCEDURE

FIRE ALARM:
(Premises open)
Call premises first at all times (maximum of 60 seconds) followed by ALL keyholder if no response the brigade will be called as per the below

Important Note: We only call the Fire Brigade as a last resort. This is due to the national policy of visual confirmation of smoke or fire from site being required for their attendance.

Should you come under **COMAH (The Control of Major Accident Hazards Regulations 2015)** or people sleep at this address known as **"Sleeping Risk"**, then we can call the Fire Brigade first to ask them to make an attendance. For guaranteed attendance under these circumstances, **please speak to your local Fire Brigade.**

(Premises unknown)
08:00-20:00 call premises first (maximum of 60 seconds) - if engaged or no answer keyholders if no answer brigade.

(Premises closed).
Keyholders informed no response,
Brigade

NB – If site or keyholders request the Fire & rescue service at any time during the activation or immediately after the activation, we will notify the fire & rescue service immediately.

HOLD UP ALARM:
Police informed

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

Telephone Confirmation for residential/domestic sites only - 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 audio/visual/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 2 – BS8243 - Types of alarm condition permitted to contribute to a sequentially confirmed HUA).

Note – If premises status is showing closed then keyholders will be informed as well as police.

DESIGNATION OF IAS SIGNALS FOR SEQUENTIAL CONFIRMATION

UNCONFIRMED ALARM:

Alarm Monitoring Policy

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

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 2 – 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

14. MIS-OPERATION SIGNAL

All Intruder and Hold-up Alarm Systems should either:

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

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:

Alarm Monitoring Policy

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.

ARC 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 ARC 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.

15. 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)

16. REDCARE LINE FAULT SIGNALS

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

Line Fault signals received on their own 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)

CONFIRMED ALARM: (i.e. Intruder Alarm followed by a Line Fault 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)

CONFIRMED ALARM: (i.e. Intruder Alarm followed by a Line Fault 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

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

17. 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)

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 14 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):
AAH notification via email or text message

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 14 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

The Garda Síochána or such other authority as the subscriber requires shall be notified of the receipt of any valid alarm signal from supervised premises at which the intruder alarm system, or part thereof, is armed. All operating procedures in force which relate to the alarm handling function shall comply with the Garda Síochána Intruder Alarm Policy.

18. AUDIBLY CONFIRMED ALARM SIGNALS

ARC currently offers facilities for the monitoring of the following types of Audio Confirmation equipment (which are all initiated by ARC (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 ARC 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:

a) 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
b) 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 ARC 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)

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

19. VISUALLY CONFIRMED ALARM SIGNALS

Installers must specify the type of equipment used when completing a Request for ARC 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 ARC 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

20. CCTV ACTIVATIONS

Request for CCTV Connection Form (our ref. OC08), a site map with location and field of view of cameras and associated detectors must be completed and received by ARC at least 24 hours before an engineer attends sites for all new CCTV connections.

For BS 8418 systems an Inventory of CCTV equipment installed must also be supplied.

NB – Any system requiring police response must have a URN and conform to BS 8418 - Installation and remote monitoring of detector activated CCTV systems – 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 read the site instructions listed on the screen and follow.
2. Having viewed the alarm frame(s) we can then accept any further alarms from the site.
3. If we do not observe any persons or suspicious activity, no further action will be taken, and the alarm will be cleared down with an appropriate comment logged.
4. If we observe suspicious activity and the system allows, ARC will use the PTZ function to take control of the cameras. (NB. We will not take control of any PTZ camera **unless** suspicious activity is observed as this could over-ride the pre-set control and therefore potentially result in missed intrusion detection).
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. 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 (e.g. 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.
11. If during the handling of an activation the quality of the image is identified as poor (e.g. due to lamp failure), or if a "failure to restart" or "restart signal" is received, please follow the customer response plan for the site.
12. If critical data required to complete the response effectively is unavailable or inaccurate (e.g. a user who is no longer valid), a fixed format notice will be issued (using CCTV Exceptions/Fault Notice form) to the Customer advising of the nature of the problem and requesting that remedial action be taken or to supply missing data.
13. Ensure all incidents are logged with details of cause of activation and action taken.
14. Video Loss Alarms - view cameras in multiple screen mode to check that all cameras are visible. If any camera(s) is not visible, please report to a keyholder immediately and record this in the logs.

21. REMOTE RESETTING OF SIGNALLING SYSTEMS

INTRODUCTION

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

BS 8473	Intruder and hold-up alarm systems – Management of false alarms
PD 6662	Scheme for the application of European Standards for intruder and hold-up alarm systems
BS EN 50131-1	Alarm Systems – Intrusion Systems – Part 1: System Requirements
BS 4737-4-4.2	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 ARC personnel if the cause of the alarm activation is determined by ARC 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 BS 8243 the police would not be notified of irregular opening or closing of the premises outside the agreed time schedules.

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 a, b or c below apply.

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

a) identification of the operator at the protected premises is not possible from the Password given by the telephone caller

b) 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

c) 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

d) 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, ARC 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.

22. CONTACT PROCEDURE

A subscriber requiring a Remote Reset must telephone the ARC on 01302 543275.

Remote Resets will ONLY be given to subscribers who can quote their PASSWORD and ARC computer search facilities will NOT be used to identify sites. The subscriber must also have a valid reason for the alarm activation as listed above.

23. RESETS GIVEN TO ALARM COMPANY SERVICE TECHNICIANS

ARC 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.

24. FINAL DECISION

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