

Thank you for choosing CIA Fire & Security Ltd to have the opportunity to provide your quotation, please find below additional information which is relevant to the alarm system.

CIA FIRE AND SECURITY LTD

STANDARD CONDITIONS AND NOTES – COMMUNICATED SYSTEMS

SYSTEM DESIGN PROPOSAL

Sequential Confirmation

The proposed installation will be in accordance with PD 6662 and DD 243

SECURITY GRADE – Site specific

(Dependent on options taken in schedule A and confirmed on schedule C-Confirmation of Acceptance)

(PD 6662 is the UK implementation of BS EN 50131).

The following System Design Proposal is for the installation of an intruder alarm system capable of generating sequential confirmation as required by the local police authority. Sequential confirmation is one means of ensuring that alarm notifications are only given to the police where there is a strong possibility of genuine intrusion. This will normally be indicated when two correctly configured detectors have activated.

A sequentially confirmed intruder alarm system is designed such that an intruder must activate two independent detection devices within the confirmed period (thirty minutes) of each other. The first activation is classed as an “unconfirmed alarm” and the second activation is classed as a “confirmed alarm”.

This sequential confirmation system is used in conjunction with an entry shock input device that uses a non latching shock/vibration device on the initial entry door.

If the initial entry door is subject to a gross attack or forced open, then only one further entry input device needs to be activated to initiate a sequentially confirmed intruder alarm.

The door entry contact must be opened within ten seconds of the shock detector triggering for the entry shock input device response to apply.

Full details of the actions taken by the Alarm Receiving Centre (ARC) on receipt of signals are given in **STANDARD CONDITIONS AND NOTES (MONITORED) - ISSUE 1 Schedule D** (Section 7 - Alarm Monitoring Response.)

Sequential Devices – Configuration

The sequential confirmation system is designed such that an intruder has to activate a detector first and then activate another detector by movement within the premises. If the activation of the second detector is within the confirmation period (thirty minutes), this will be passed to the ARC as a confirmed alarm. The system has been designed to minimise any potential loss.

The confirmation time will not re-start if the first detector to report an alarm condition reports again within the confirmation time.

Input Device Descriptions

Circuits/Input Device Descriptions are contained in Specification.

Control and Indicating Equipment

The control and indicating equipment is described in the System Design Proposal /Equipment Listing.

Features of the system

Back up Power Supply

Yuasa rechargeable batteries are incorporated within the control panel to perform as a standby source of power in the event of a mains power failure. Whilst the mains power is operating correctly these batteries are being trickled charged. The control panel battery will maintain the system in a quiescent state for a minimum of twelve hours for grades 1 & 2 and 24 hrs for grade 3.

Audible Warning Devices (Sounders)

The Armour-flash external bell box is a metal zintec coated housing with foam protection and an inbuilt sounder and strobe with an S.A.B. sealed circuit board complete with Ni-Cad battery.

Anti - Tamper Protection

All control equipment, external sounder and circuits including sensors, contacts, hold up alarms etc. have their own anti tamper circuits.

Should an attempt be made to remove any lid or cut any cable in the day (unset) state a local alarm will be generated. Should a cable be cut or a lid removed with the system set a full alarm will be generated.

Reinstatement Signals

Where confirmation technology is incorporated and a detector triggers, a first indication (unconfirmed) intruder signal will be transmitted to the alarm-receiving centre. **This will not be processed as a confirmation signal.** An activation from another alarm input of the system within a thirty-minute period would be processed as a confirmation signal.

The intruder alarm system is designed to re-arm if a first indication intruder (unconfirmed) alarm is not followed by a second indication (confirmation signal) within any thirty minute period. This reinstates the system to an initial "no indication" set condition.

If any device indicates a fault condition at the thirty minute re-arm stage, then the input affected will be omitted by the control panel which will send a re-instatement signal to the alarm receiving centre advising them that an input is isolated for that setting period.

Alarm Transmission Path Check Signals

PD 6662 requires routine test signals to be sent to the Alarm Receiving Centre. The interval between test signals would normally be 25 hours (dependent upon the grade of system specified). The telephone call incorporating the test signal would be chargeable at BT national rates which for a Grade 2 system could equate to £7.50 per quarter.

In some cases it may be possible to add the test call telephone number to a 'Friends and Family' lower rate calls package. For your test call telephone number please speak to the engineer when on site or speak to our office on 01285 651025

Intentional Pre-Alarm Time Delays

An intentional pre-alarm time delay is incorporated in the Control and Indicating Equipment to avoid generation of false alarms during setting and un-setting of the system.

The delay incorporated in your system is set initially at thirty seconds. This may be altered to shorten or lengthen the period allowed to facilitate setting/un-setting.

Means of Setting and Un-setting

Setting the System

Setting of the system is in accordance with Clause 6.3d of DD243 and is achieved by presenting the key tag to the control panel or keying in a code number in the control keypad then leaving by the final exit door. A confirmation sound will be given on successful completion of setting.

Un-setting the System

Un-setting of the system is in accordance with Clause 6.4.5 of DD243 and is achieved on opening the entry door and un-setting the system by presenting the key tag to the control panel.

There is a timed entry procedure not exceeding 45 seconds and when the initial entry door is opened, notification of any alarm is delayed until expiry of the overall entry time.

If an alarm occurs during entry, forcing an entry and/or as a result of the expiry of the overall entry time, the alarm will be notified as an unconfirmed alarm. On opening the entry door, the system can then be unset by presenting a key tag to the keypad within the allotted overall entry time.

Forced opening of the initial entry door followed by the activation of a further detection device not on the entry route should generate a confirmed alarm signal.

If you activate two programmed detector devices outside the entry route this will generate a confirmed alarm.

Engineer Access to Control and Indication Equipment

The current code of practice requires engineer access to the control and indication equipment (CIE) to be controlled.

Access to the CIE for routine maintenance purposes must be authorised by the user.

This authorisation can be given on each visit in which case the user would need to enter their access code at each stage of the access entry and exit processes. **This would mean that, if a user were not present, maintenance would not be possible.**

Failure to obtain the necessary access authorisation would prevent our engineer from carrying out routine maintenance. Due to the obvious costs involved it CIA will invoice any unproductive time resulting from abortive visits.

Normally it is preferable for the user to authorise unaccompanied engineer access. Granting the appropriate access permission on the CIE keypad can do this. Our engineer will guide you through this process.

You will be asked to confirm your agreement to this authorisation by countersigning our Hand Over Form F11(l) and Service Contract F43 (l)

Fire Detectors

The integration of one or more fire detection devices does not constitute a fire detection system under the terms of the Fire Safety Order coming into effect April 2006. From that date a URN must be obtained before any notifications can be made to a fire authority control centre. To obtain the URN the fire detection and alarm system must comply with BS 5839 and be from April 2007 be certified by an accredited company.

Lightning Protection

Lightning damage is not covered by your guarantee. Lightning strikes on the national telephone system frequently cause damage to electronic equipment connected to the telephone networks.

Lightning protectors are now available to protect your communicator from the effects of lightning. Should you wish to have this item fitted the cost is indicated in our quotation.

Please note that lightning protection for your communicator would not give protection against damage to your premises or power supply as a result of a direct lightning strike. A lightning strike can result in serious damage to electrical installations including your intruder alarm system wiring and components. **General protection would not be provided by the communicator protection.**

On very rare occasions, following a severe electric storm, you may have problems with your telephone system particularly if you suspect that your house has been subjected to a direct lightning strike. In these circumstances we recommend that your intruder alarm control panel is checked before calling your telephone service provider. Although our visit will be chargeable it could avoid significant service call out charges from your telephone service provider.

Access for Inspection

Should our estimate be accepted then the purchaser agrees that the installer and NSI/NACOSS may be allowed access for the installation, maintenance and inspection of the system.

Customer Damage

CIA is not liable for damage caused by customer action or resulting from customer misdirection.

Intruder Damage

CIA is not liable for damage to equipment caused by intruders or attempts to disable the system in the course of an attempted break in.

Customer Interference

CIA is not responsible for damage resulting from interference or inspection of the system by the customer.

Noise Pollution

Customer's attention is drawn to the need to minimise noise pollution and external sounders are designed to curtail their operation after 15 minutes.

Training

You will receive training on the operation of the system including methods of cancelling accidental operation of the alarm.

External Warning Devices

Owners of intruder alarms causing annoyance under the terms of the Control of Pollution Act may result in prosecution. Your external sounder should be programmed to cut out after 15 minutes.

Data Protection Act

In accordance with the Data Protection Act 1984 personal information relating to you and your key-holders in connections with the security system may be held on a computer. Please ensure that relevant names and addresses are current.

Premium Rate Telephone Numbers – SMS Text Messaging Service

Where your system incorporates text message notification of activations the communications panel is programmed to access its host computer twice a month to keep the bureau telephone number listing up to date. During commissioning and servicing it is necessary to carry out a CHC (Castle Host Computer) call.

These calls are made to a premium rate number and as the duration of each call is low the charges are minimal but will appear on your telephone bill.

Text messages will be charged at normal text messaging on your landline.

Changes to Property and Contents

It is the clients responsibility to inform CIA Fire & Security Ltd of any alterations made to the property or additions to its contents that may affect the functionality or effectiveness of the intruder alarm system i.e. erection of stud wall, increase in value of items in room.

Quotes Made From Architects Drawings

Should this quotation be provided using a set of architects drawings and therefore a full site risk assessment in accordance with PD6662 was not conducted CIA Fire & Security Ltd is not liable for goods within the property. This quotation is provided to cover the volume only of each room and not its contents. Therefore, it is the client's responsibility to inform CIA of any known health and safety risks/hazards and any specific items they require protecting.

STANDARD CONDITIONS AND NOTES (MONITORED) SCHEDULE D - ISSUE 1

General Conditions

Our quotation is based on installation to PD 6662, and National Security Inspectorate/ National Approval Council for Security Systems (NSI/NACOSS) requirements. Where applicable for installations incorporating confirmation technology the system meets the requirements of DD243.

Environmental Requirements

NSI/NACOSS NACP 2 clause 6.4 states that where a security system incorporating an audible alarm is installed the owner should notify the local police and environmental health authority within forty-eight hours of the system coming into operation.

NACP 2. Clause 6.5 states that any security system fitted with an audible alarm should have a cut off time not exceeding 15 minutes. Where an alarm is fitted at

the insistence of their Insurers, customers should ensure that the curtailment of the audible alarm after the agreed period is acceptable.

Police Response

NSI/NACOSS Code of Practice NACP 2, Customer Communications, clause 6.3 requires us to advise you that a monitored alarm system that passes three false alarms to the police in one year will result in the police withdrawing their response. This would leave you without the benefit of notification of the Police. This withdrawal will initially be until a three-month trouble free period has expired. However if the situation is not resolved within six months, the police Unique Reference Number (URN) could be withdrawn. Should this occur it is the responsibility of the owner of the system to notify his insurer and obtain guidance.

Insurance

You should for insurance purposes pass this system design proposal to your insurance company.

Recognition

CIA Fire & Security Ltd are approved as installers by all local police authorities including Gloucestershire, Wiltshire and Thames Valley police.

CIA Fire & Security Ltd are a **NSI /NACOSS GOLD** registered installer and our procedures conform to their standards.

Our business procedures comply with BS EN ISO 9001 2000.

CIA Fire & Security Ltd Liability Cover

We are insured for PUBLIC LIABILITY limited to £ 5,000,000, EMPLOYERS LIABILITY limited to £ 10,000,000, PRODUCT LIABILITY and WRONGFUL ADVICE limited to £5,000,000.

Back Up Service

A twenty-four hour call out service is provided. This service is manned during office hours by our technical support team and out of hours by our SIA licensed Alarm Response Operatives, on-call alarm engineers and supported by senior management.

Maintenance Service

Monitored systems require six monthly services.

The service charge is paid annually in advance. After each service you will be advised of the engineers findings in a copy of his report should it be requested.

If the annual maintenance of the alarm is cancelled during the guarantee period, the guarantee is null and void and an increased call-out charge may be incurred.

Call out Charges

Where applicable, call out charges will be made. In addition mileage charged per mile will apply for each additional attendance outside the agreed service requirement.

Call out charges will apply if the fault is not the fault of CIA Fire & Security Ltd or the call out results from an attempted burglary.

System Ownership/Guarantee

The complete system is wholly owned by the client and guaranteed for two years on settlement of installation invoice.

Our two-year guarantee is subject to the system being maintained under our service contract.

Smoking

CIA Fire & Security Ltd operates a no smoking policy.

ALARM TRANSMISSION OPTIONS

INTRODUCTION

As advised during your initial enquiry, there are several options available for the monitoring of your system, all of which would be linked to our Alarm Receiving Centre – Southern Monitoring Services

DIGITAL COMMUNICATION

Digital communication is installed within the control panel. This equipment can communicate up to four signals to the central station. The drawback with a digital communicator is that if the BT line is lost there is no way for the monitoring station receiving signals from the alarm system, therefore the alarm system reverts back to an audible only system.

The Digital communication is compatible with any standard telephone line. However please bare in mind that it could be possible to have the line jammed. In some cases it is possible to program the communicator so it cannot be jammed, if this is not possible a dedicated line is required with incoming calls barred.

PD 6662 requires routine checking of the communication path. This is generally done by sending a daily test signal to the Alarm Receiving Centre. This signal should be of short duration and is chargeable at BT national rates.

REDCARE COMMUNICATION (Domestic or Commercial)

Redcare is connected to an Alarm Receiving Centre via a phone line, Redcare continuously checks that the phone line is there and unlike the digital communicator it will notify the Alarm Receiving Centre within seconds should there be a problem. This means that your alarm signalling can never be compromised without the knowledge of the Alarm Receiving Centre.

Redcare's unique technology works using a BT landline or broadband connection to send an unbroken pattern of two-way signals from your premises to your Alarm Receiving Centre. If for any reason these signals are interrupted Redcare will deliver a warning signal to your Alarm Receiving Centre who will summon the emergency services, and or key-holder as required.

What is the Redcare Bock Terminal?

The RedCare block terminal (BT92A) product is specifically designed for the alarm security market and the termination of a RedCare connection at the customer's premises.

The UK security signalling market has a long standing requirement for a hard wired block installation (tamper protection). This means there are no connection points at which the alarm signalling service can be accidentally or maliciously unplugged or disconnected enhancing the security of the alarm installation. This is achieved by a BT engineer cabling and connecting the RedCare block terminal directly to the PSTN line.

RedCare block terminal benefits

- Convenient demarcation and connection point for the alarm installer
- It is a hard wired installation maximising security by reducing likelihood of accidental or malicious disconnection, avoiding inadvertent disconnection during customer usage or customer / 3rd Party provision of additional services on the line
- Reduces the false alarm potential of the installation
- Co-ordinates installation with the RedCare signalling service
- Quality installation by BT engineer
- Automated end-to-end testing of the installation and RedCare service by the BT engineer.

REDCARE GSM COMMUNICATION (Domestic or Commercial)

Redcare GSM works in parallel with the standard Redcare unit but with an additional radio path. Should one of the paths be lost to the control panel the second will be able to communicate an alarm activation. Should both paths be lost the police will be requested to attend site.

DUALCOM COMMUNICATION

Dualcom is a signalling device that combines a digital communicator and radio path, should the radio path be lost to the control panel signals can be sent via the telephone path, should the telephone path be lost signals can be sent via the radio path.

If one of the signal paths fails and an alarm is received shortly afterwards on the other signal path this is treated as a confirmed alarm. Similarly a failure of both systems is classed as a confirmed alarm. In either case the ARC will notify the police and key-holder accordingly. Line fault failure is indicated at the control panel.

Note: Should the radio link be lost then the telephone path is lost, there is no way for this telephone loss to be signalled to the monitoring station.

DUALCOM GPRS

Dualcom GPRS, from CSL Dualcom Limited, is an intruder alarm signalling device that uses both the Vodafone network and your telephone path to transmit intruder and personal attack signals at high speed. Once the alarm is confirmed as genuine, police are notified. Utilising two signalling paths ensures that Dualcom dual-signalling will always have a back-up path in the event of an accidental or deliberate fault on either path.

CIA cannot guarantee the above options are suitable with existing telephone lines prior to installation, unless a site test is made.

CIA Fire & Security Ltd offer a professional Keyholding and Alarm Response service to take the place of or assist your key-holder in attending site. Details of this service are available on request.

IMPORTANT

Your attention is drawn to the fact that failure or compromise of a single path signalling (1 or 2 above) cannot be passed to the police. While the failure persists, subsequent alarms cannot be signalled to the alarm receiving centre and passed to the police.

SIGNALLING & GENERAL NOTES

Where applicable your system will be designed to generate the following additional signals: -

Open/Close (not available on digital communicators)	Signal sent to ARC each time final entry/exit procedure is completed.
Set/Unset	Signal sent to the ARC each time that the system is set or unset.
Abort	If an abort signal is received within the alarm processing period (120 secs) action is cancelled
System Restoral	If system restore is received within the alarm processing period (120 secs) , action is cancelled
Confirmation signals	On receipt of a first (unconfirmed) alarm is received at the ARC only the key-holder will be informed. If a further alarm is received within the confirmation period (thirty minutes) of the first alarm, it is classified as a confirmed alarm and the police and key-holder will be informed.
Reinstatement	If a second alarm is not received within the confirmation period (thirty minutes) the system is reinstated. This does not remove the alarm condition and on un-setting there will be an indication at the control panel of the alarm condition indicating that a reset is required.
Telephone	During certain times of the day any alarm condition may also be verified by a telephone call to the premises.
Hold Up	Signal sent to the ARC each time a deliberately operated device is operated to indicate an impending personal attack.
Fire	Signal sent to the ARC each time a specifically fire detection device integrated into the system is activated.
Line Fault	Signal sent to the ARC by the telephone line provider each time the provider detects that the line dedicated to communicate with the ARC is has been interfered with.
Communication Path Test Signals	Automatic Signal sent to Alarm Receiving Centre to verify that communication path is functional
Miscellaneous Signals	Input omit rearm - giving facility to recommence confirmation period. Mains Failure - Facility to advise of mains failure or low battery

	Trouble Alarm - Facility to notify of faults or environmental alarms
--	--

GENERAL NOTES

1. If the property is a monitored system it will not be on police coverage for a minimum of 14 days after completed hand over sheet is received and on receiving details of two key-holders within 20 minutes of the property (or CIA as key-holder).
2. In accordance with the Association of Chief Police Officers (ACPO) Security Systems Policy your local police make a charge for issuing URN's (£55). A URN is a Unique Reference Number used to identify and locate a property.
3. Should you not use CIA's key-holding service then two key-holders are required within 20-minute travelling time of the property. If the property is monitored the police will not issue a URN until this is arranged.
4. The alarm receiving centre will only authorise two resets in a 30-day period if the alarms were policed, on the third policed request for a reset the monitoring station will refer the customer to CIA Fire & Security Ltd to investigate the cause of activations.

FALSE ALARM POLICY – COMMUNICATED SYSTEMS

False Alarm Policy Statement

It is CIA's intention to reduce false alarm activation's by targeting three areas of installation.

1. End user training, simplifying operating procedure.
2. Continually ' Up spec ' installation procedure/equipment.
3. Use performance information to monitor products.

In addition we: -

- Use Castle Care-Tech control panels where possible for ease of use by the end user.
- Use screened cable to be used throughout.
- Standardise on Dual passive microwave detectors.
- Earth out all unused cores.
- Analyse all false alarm information and liaise with manufacturers re: solutions.
- Fit communications lightning protection where client agrees.
- Use sequential, audio or visual verification.

STANDARD ALARM MONITORING RESPONSE

General

A specialised Alarm Receiving Centre on behalf of CIA Fire & Security Ltd carries out monitoring of your intruder alarm system. The Alarm Receiving Centre

standard response to alarm signals is detailed in the tables contained within this section of the contract documents. The action taken by the Alarm Receiving Centre will be as indicated unless the end user has instructed otherwise.

In the event that more than one alarm signal is received at the same time, only the highest priority alarm will be actioned.

Filtering Policy (when an alarm system activates)

The following techniques are used for filtering intruder alarms in accordance with the Association of Chief Police Officers (ACPO) Policy 2000, NSI/NACOSS Code of Practice,

NACP 14, and Code of Practice DD 243 - Installation and Configuration of Intruder Alarm Installations Designed to Generate Confirmed Alarm Conditions.

1 - Mis-operation Signals

All systems shall either

- a) **Be capable of generating a secondary signal to indicate that the alarm system has been miss-operated**

Or

- b) Send an unset/set (open/close) signal

Where the Alarm Receiving Centre is unable to identify whether the system is set/unset (open/closed) they will action it as “closed”.

The Alarm receiving Centre will then respond to alarms in the following way:

Miss-Operation by Abort or Open Signals

This is by far the most cost-effective route for customers with Digital Communicators and is the recommended option for residential systems.

A miss-operation signal will result in us not calling the police and aborting all actions.

A miss-operation signal may be transmitted in a number of different ways, depending on the controlled equipment installed.

A miss-operation signal may be sent by a deliberate action by the end user (abort button, entering a code etc) or by un-setting the system within 120 seconds of activation.

The Alarm Receiving Centre (ARC) response will then be:

Type of Alarm	Action taken by ARC
Intruder Alarm coupled with mis-operation/abort signal within 120 Seconds.	No action taken.

2 – Hold Up Alarms

Type of Alarm	Action taken by ARC
Hold Up	Police & Contacts

3 – Fire Alarms

Type of Alarm	Action taken by ARC
For Fire detection inputs linked to intruder Fire Alarm	Site, (Contacts if no reply)

4. - Intruder Alarms

Type of Alarm	Action taken by ARC
Unconfirmed Intruder Alarm	Premises (Contacts if no reply)
Confirmed Sequential Intruder Alarm when closed within re-arm period or audio/visual verification	Police (as confirmed) and contacts.
Unconfirmed Intruder Alarm followed by an Open or Abort signal within filter period of 120 seconds	No action taken
Sequentially Confirmed Intruder Alarm received within filter period followed by Open or Abort signal within filtering period	No action taken

NOTES:

All new intruder alarm systems installed within an ACPO police authority area that requires a police response and systems that have had police response withdrawn but now require police response reinstating must incorporate confirmation technology.

All intruder alarm signals received from sequentially confirmed intruder alarm systems within premises in ACPO Police authority areas are held for 120 seconds in order that they may be aborted or confirmed by a second detector.

Subject to formal written agreement clients may specify alternative response to the first alarm signal e.g. Take no action on first signal.

Where CIA are not key-holders, the ARC will make every attempt to make contact with key-holders provided over a 30 minute period. If it is not possible to notify a key-holder no further action will be taken.

Exceptions to the above may be made however these must be confirmed in writing.

TYPES OF CONFIRMED ALARM

5.1 Sequential Alarms (Second Input Reporting)

Sequential alarms are one of the simplest confirmation technologies. The Alarm Receiving Centre (ARC) just needs to know that two independent detectors or two detectors of different technologies have activated within the protected premises.

Signals are held for a minimum of 120 seconds in order that the alarm may be aborted or confirmed.

Should a confirmed intruder alarm signal be received within the alarm filter period of the initial alarm, on expiry of the initial filter time the alarm is presented to an operator for action as a confirmed alarm.

Should the end user send a miss-operation signal or a signal to indicate the system is unset prior to any action by the ARC the alarm will normally be automatically aborted.

Alarm systems incorporating sequential confirmation are set to re-arm within a time window (30-60 minutes) following initial activation to prevent the transmission of a confirmed alarm signal and to prevent the ARC from carrying out an incorrect action on any subsequent activation.

5.2 Audio/Visual Alarms

On contact with the Audio or Visual System, the system confirms the identity of the premises to the ARC.

Should a sound be heard or person be seen the ARC will treat the activation as a confirmed alarm.

The ARC will not use discretion if a sound or person is seen - *They will Police.*

NOTE:

To minimise the incidence of an incorrect response by the ARC it is essential that the Alarm Listening Devices or Imaging Devices maintain the same area of coverage as the intruder detection that caused the alarm incident.

Under normal circumstances the ARC undertake the following time guidelines:

Pre-alarm	10 seconds
Post-alarm	20 seconds
Real time	30 seconds

6. No Response/Line Fault Verification

IMPORTANT – Your attention is drawn to the fact that failure or compromise of signal path signalling cannot be passed to the police. While the failure persists, subsequent alarms cannot be signalled to the alarm system and passed to the police.

No Response Alarm Signals will not attract a police response unless they precede or follow an Intruder Alarm Signal.

Systems that monitor NO Response/Line Fail also transmit open and closed signals to the ARC to ensure that the correct response to communication failure is carried out in accordance with clause 6.4.2 of BS 5979.

The ARC action plans for a No Response/Line Fault on **Dualcom, Dualcom GSM, RedCARE, RedCARE GSM, RedCARE ISDN and RedCARE Serial** systems are:

Type of Signal	Action taken by ARC
Single No Response ⁽¹⁾ (RedCARE No Response Signal, BT Line Fail, Paknet Comms Fail or GSM Comms	Premises or contacts and CIA (if required)

Fail)	
Any combination of No Response, Line Fail or Intruder Alarm when the system is known to be open or alarm combinations are not received within the same set period ^(2,3 & 4)	Premises or contacts and CIA (if required)
Outstanding No Response Alarm in an un-restored state followed by an intruder alarm received within the same set period and the system is recorded as closed ^(1,2,3 & 4)	Police (as confirmed) and contacts
Outstanding Intruder Alarm in an un-restored state followed by No Response Alarm within the same set period and the system is recorded as closed ^(3 & 4)	Police (as confirmed) and contacts
Outstanding No Response Alarm in an un-restored state followed by No Response Alarm via an alternative signalling path received within the same set period and the system is recorded as closed ⁽⁵⁾	Police (as confirmed) and contacts

NOTES:

1. RedCARE may generate network control messages to inform the ARC that a fault exists on a line or a single STU. In such case, the ARC may elect to inform contacts and/or premises.
2. The system must be dual signalling for an Intruder Alarm to be received following a No Response Alarm.
3. For the action to be carried out correctly in the event of a No Response Alarm coupled with an Intruder Alarm, the alarm system must send “restores” on all intruder alarm channels.
4. Upgrade of activations to a policed event must be agreed formally with CIA who will instruct the ARC accordingly.
5. The system must be dual signalling for two No Response Alarms to be received via alternative signalling paths.

7 – Systems with Opening and Closing Time Schedules

The ARC response for systems where opening and closing time schedules are in place will be:

Early Open (open more than thirty minutes before scheduled opening time)	Premises or contacts
Fail to close (close more than thirty minutes before scheduled closing time)	Premises or contacts

NOTES:

Alarm filtering is not applied to Sequential Confirmed Intruder Alarm Signals received at least 30 minutes after latest closing or more than 30 minutes before agreed earliest opening time and the alarm has been set for at least 15 minutes.

8 – Miscellaneous Signals

The ARC response for miscellaneous signals will be:

Input Omit Rearm	Inform keyholder that system has been re-armed and confirmation period has been recommenced
Mains Failure/Low battery	Premises or contacts
Trouble Alarm	Advise keyholder using site specific instruction
Environmental Alarm	Advise keyholder using site specific instruction
Automatic Test Signals	Log only CIA to assess daily report

D8. REMOTE RESET(RESTORE) FACILITY

The end user will be fully instructed in the procedure for carrying out a remote reset and the circumstances under which a remote reset can be given.

Procedure

Following receipt of a signalled alarm condition by the Alarm Receiving Centre (ARC), the system may be reset remotely by the Alarm Receiving Centre (acting in conjunction with the user of the alarm system in attendance at the protected premises) and authorised by the Alarm Receiving Centre in accordance with Section 10 of BS 8473:2006

Resetting in accordance with above shall only be authorised by the ARC if the following conditions are satisfied:

Should the ARC receive an immediate abort signal or contact site, the client may request a remote reset.

A remote reset can be given in the following circumstances:-

Restoring should only be carried out by either of the following:

- a) by a CIA engineer at the premises
- b) by the user at the premises acting in conjunction with the Alarm Receiving Centre (ARC)
- c) remotely by electronic signals in conjunction with the user and authorized by the duty officer at the ARC

For alarms which have not been passed to Police:

Where agreed, for systems incorporating confirmation technology, the customer may reset unconfirmed alarms conditions without reference to the Alarm Receiving Centre or CIA Fire & Security Ltd.

For alarms which have been passed to the Police the following conditions apply:

- a. When end user agreement has been obtained and authorised by an agreed security discipline (by exchange of predetermined code words or numbers).
- b. The cause of the signalled alarm condition has been clearly described by the end user to the Engineer or the duty operator at the Alarm Receiving Centre and the description given is consistent with the alarm condition having been caused by client error; or the cause is known not to be with the alarm system.
- c. The description of the cause of the signalled alarm condition is consistent with there being no requirement for an engineers visit.

Note: It is not permissible to remotely reset an alarm that has been extended to the Police if the number of policed alarms has exceeded one within the last twelve months.

In these circumstances an engineer must attend site to investigate the cause of the activation.

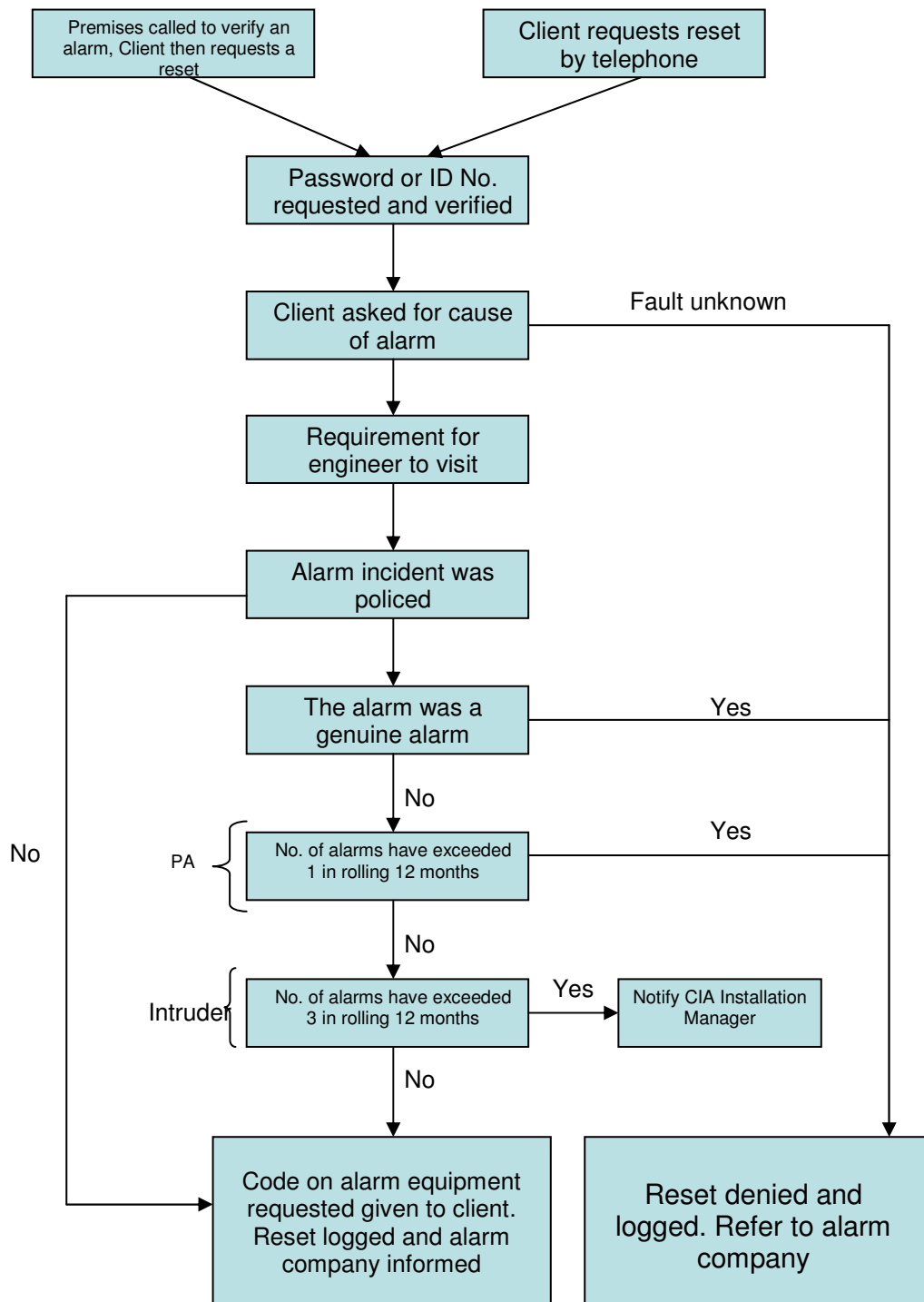
System Reset/Restore

The user will be asked to supply the number displayed on the keypad and their password and in return is given an anti code for entry into the keypad.

In the case of a genuine alarm or genuine confirmed alarm, you should be aware that your insurance cover could be invalidated if a service technician's visit does not take place and the system is subsequently found to be not in full working order.

A remote reset cannot be given if the police have been mobilised until after the police have attended. Where remote reset is denied, the Alarm Company's Service Technician will visit the protected premises for the purpose of inspecting the installation, corrective maintenance and/or educating the user as appropriate.

REMOTE RESTORE FLOWCHART



KEYHOLDING

Client Supplied Keyholders

For communicated systems you need to provide the names and telephone numbers of at least two people living within 20 minutes of your property who will be your key-holders.

Key-holders must be able to use your alarm, hold the keys for your property and will know the code or have a tag to set/unset your alarm. Your key-holders also need to know your security identity password.

Failure of key-holders to attend within twenty minutes when requested on three occasions in a rolling twelve month period, will result in the withdrawal of police response for a three month period.

CIA Fire & Security Ltd Keyholding and Alarm Response

The Association of Chief Police Officers (ACPO) Security Systems Policy, defines criteria for police response. In April 2006 three false calls within a rolling 12 month period will result in withdrawal of police response until a three month period free of false calls has elapsed. Further false calls or a failure to remedy the problem within six months could result in the police withdrawing your URN. You would then be required to upgrade your system before a new URN could be applied for. This could involve significant expense.

A key point in the policy states that the initial unconfirmed intruder activation will not be passed to the police but to your first key-holder. **This may result in the key-holder attending site without police presence.**

CIA are therefore offering a key-holding, alarm response and patrol service, manned by our own trained personnel. These personnel can assist a key-holder on site or take the place of a key-holder and attend activation's, access the premises, identify the cause of the activation and where necessary liaise with the police, fire brigade and the alarm engineers without unnecessarily inconveniencing staff or friends.

We are pleased to offer this unparalleled service at present within a 15mile radius of our town centre offices.

Costs of the key-holding service are laid down in the options in Schedule A - Installation Chargeable Options - section D.

To take up this option please indicate on the confirmation of acceptance form (Schedule C) Option C.

PREVENTING FALSE ALARMS – POINTS TO REMEMBER

INTRUDER ALARMS

- 1) The alarm installation should be operated only by persons who have been trained in its operation. If there is any uncertainty about the correct operational procedures.
- 2) Before leaving the premises check that all doors and windows are physically secured. A walk around the protected area is the only effective way of doing this properly.
- 3) Ensure that detection devices are not obstructed. In particular be careful that infrared beams and space detectors are not obstructed by stock or other items.
- 4) Keep sensors free from cobwebs and spiders etc - **this is a classic false alarm cause.**
- 5) If space detectors are used do not introduce sources of heat, movement or sound into the area protected by these detectors without informing the alarm company. In hot weather please remember to shut windows and turn off fans in rooms where there are detectors - **this is a frequent problem.**
- 6) Remember to put all pets in the relevant rooms before setting your alarm.
- 7) Always follow the entry/exit procedure agreed with the alarm company. Entry through any door other than the one designated is not to be allowed. Switching off the alarm system is always the first task on entry.
- 8) Before entry, ensure that all the keys/tags necessary to enter the premises are readily available and where applicable code numbers are known.
- 9) Inform the alarm company of any alterations to the premises that might affect the alarm system. Do not permit people other than employees of the alarm company to make changes to the alarm system.
- 10) Treat the alarm system with care. Wiring and detection devices can be accidentally damaged or moved. Should this occur inform the alarm company immediately. If you know work is to be carried out and that sensors etc. may need moving, please let us know in advance.
- 11) After a false alarm check the system carefully and, if possible, note the cause of activation. Inform the alarm company engineer of the believed cause of the activation immediately.
- 12) Make sure that regular maintenance checks are carried out by your alarm company. Remember that excessive false alarms will normally result in police response being withdrawn.
- 13) When a problem arises remember to contact CIA on 07860 910055. This is a paging service, leave your name and telephone number and the engineer will call you straight back.
- 14) If you have a monitored system and make a mistake immediately phone the monitoring station using the telephone number on the sticker on your keypad and quote your password. This will ensure that the Police are not called. If CIA are a key-holder please wait for them to make contact with you before you leave the premises.
- 15) Your burglar alarm is a serious attempt at preventing crime. Be responsible in its use. Ensure that CIA are kept fully up to date with any changes to key-holders etc.

- 16) Do not give unaccompanied access to the premises without full training on the operation of the system and the password procedure. Passwords can be altered by formally informing us of the change.
- 17) **Lightning protectors** are now available to provide limited protection for your communicator from the effects of lightning as lightning damage is not covered by your guarantee. Should you wish to have this item fitted the cost would be £30.30 plus VAT. (see also General Notes & Conditions). For more comprehensive lightning protection please ask for a separate quotation.
- 18) For Redcare users there is an **added** service that BT provide in the event of a line disruption. This service is called Total Care for which there is an additional cost. Should you be interested please let us know. This guarantees repair within 4 hours.
- 19) Most intruder alarm systems require a mains supply. If the electricity supply to your system is disconnected for more than 4 hours contact CIA as soon as possible.

HOLD-UP ALARMS

- 1) A hold-up device should only be operated to summon urgent assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that area.
- 2) The hold-up device is for the personal safety of staff on the premises. Misuse results in the loss of police response to this facility. The guidelines in the table below should assist in the avoidance of false activations.

INCIDENT	RECOMMENDED ACTION	NOTES
A threat of current or imminent physical danger to staff on the premises.	Press the hold-up device	This is the intended function of a hold-up device or "personal attack" button
Theft of property or fraud with the suspects still on the premises e.g. petrol station drive offs, shoplifting, suspicious persons.	Dial 999 and give details (unless to do so would provoke an attack in which case activate hold-up device.	The hold-up alarm should not normally be used for this type of incident.
Theft of property or fraud with the suspects no longer on the premises.	Contact local police by non-emergency means	If the suspects have left, then the incident is no longer an emergency.
Incident outside the premises.	Dial 999 and give details (unless to do so would provoke an attack in which case activate hold-up device.	The hold-up device is specific to the premises.
Note: The use of the hold-up device provides the police with very little information. A phone call can help with details of a crime such as descriptions etc.		

- 3) Always contact CIA if any building or electrical work is being carried out that could result in cable or equipment damage.
- 4) Put labels on the hold-up devices to identify them e.g. "POLICE HOLD UP".
- 5) Do not attempt to remove the hold-up device from its mounting.
- 6) In domestic environments, hold-up devices should be out of reach of small children.
- 7) Portable hold-up devices should be accounted for at all times and users properly trained in their use.

CONTRACT TERMS & CONDITIONS

1. All prices quoted are subject to the following terms and conditions. The company reserves their rights to, in the event of changes to the regulations affecting specification and/or the cost of equipment, alter the quotation specification and/or cost. The client will always be consulted.
2. VAT will be added at the appropriate rate at the time of invoicing.
3. Any items supplied by the company found to be defective due to bad ownership or faulty components, will be repaired free of charge provided the company is advised of any defects within a period of three months from the date of failure and within the 2 year Guarantee period. After the date, all equipment that develops a fault will be replaced but materials and labour will be invoiced.
4. Accounts strictly net-seven days from date of invoice.
5. Subject to the provision for repair in respect of bad workmanship or component as set out above.
6. No liability shall attach to the company in respect of consequential loss or damage howsoever arising due to the failure or non-performance of the equipment or any part thereof.
7. In any case of litigation English law shall always be deemed to apply and the company will only be responsible for the value of goods supplied.
8. Liability in all cases howsoever arising is limited to the purchase price of goods supplied only.
9. Notwithstanding the installation of components or equipment on the purchasers property ownership of goods does not pass until payment has been made in full and the purchaser hereby permits and authorises the company to enter upon its land for the purpose of removing the components or other equipment installed by the company in respect of which an account remains outstanding and the company shall not be responsible or liable for any damage occasioned by the removal of such components or equipment.
10. The system is NOT complete until handed over officially by the engineer and hand over sheet signed by customer.