Securitas Operation Centre

Operational and Administrative Manual

Contents

1. Introduction

1.1 Scope

This booklet and the material recorded herein is the property of Securitas Security Services UK Ltd and shall not be used or copied without our permission. Companies who connect monitored services with us are permitted to use extracts from this document to form their own terms and conditions of service to their customers.

This booklet sets out necessary information regarding the administrative and operational services provided to Companies and End Users for the provision of monitoring services and should be read in combination with our standard terms and conditions. Although we have attempted to cover all aspects of service provision, the references cannot be extensive and our trained staff are always available to assist you further.
Prior to connecting systems to our SOC you will need to have agreed a monitoring contract with us.

Alarm Responses stated throughout this booklet are in accordance with the ACPO / NPCC Policy, ACPOS Policy and the industry standards noted under "Normative References" below. Reference to pre-ACPO 2000 Alarm Response Plans.

Throughout this booklet "Company" refers to the organisation that provides service and maintenance for alarm systems or who pays for the monitoring service for example Alarm Company, National Account or End User, see Glossary for further definitions and abbreviations used throughout this booklet.

Our commitment to the continual improvement of our quality systems and procedures to meet the needs of our clients and to reflect changes in industry requirements means the contents of this document are subject to change without notice.

1.2 Normative References

This booklet has been formulated from Industry Standards and is intended as a guide to Companies who connect monitored services with our Alarm Receiving Centre (SOC). This guide is based on, and should be read in conjunction with, the following reference documents:

- National Police Chiefs' Council
- ACPO (Association of Chief Police Officers) Security Systems Policy
- Police Scotland - Security Systems Policy
- BS5839 Fire detection and alarm systems for buildings
- BS8473 Code of practice for management of false alarms
- BS EN 50518 Code of practice for remote centres receiving signals for security systems
- BS7858 Code of practice for security screening of individuals employed in a security environment
- BS8484 Code of practice for the provision of lone worker device (LWD) services

- BS8243 Code of practice for the Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions
- BS EN 50131-1 Alarm systems - Intrusion systems - Part 1. General requirements
- BS EN 50131-6 Alarm systems - Intrusion systems - Part 6. Power Supplies requirements
- BS EN 50136 (All parts), Alarm Systems - Alarm transmission systems and equipment
- PD6662 Scheme for the application of European standards for intruder alarm systems
- Data Protection Act

For alarm systems installed in Southern Ireland the following documents are also referenced:

- IS228 Monitoring Centres for Intruder Alarm System
- SR25 SOC's Alarm Handling Procedures
- SR41 Electronic Security Services – Monitoring Services
- Garda Siochana Policy on Monitored Intruder Alarms
- PSA 33 Licensing Requirements Alarm Monitoring Centres

Installing and maintenance companies should also ensure that the technical requirements of control panel manufacturers and monitoring transmission providers are complied with.

1.3 Registration & Approvals

Our Alarm Receiving Centre operates as trading divisions of Security Monitoring Centres Limited, registered in England No. 318215.

The Alarm Receiving Centre (SOC) is assessed under the National Security Inspectorate (NSI) Gold Scheme as a Category II SOC for the monitoring of Fire and Intruder Alarms, monitoring of Lone Worker Devices and registered with the Private Security Authority in Ireland for the monitoring of Intruder Alarms and CCTV Alarm Systems.

For further details refer to the certificates of approval within section 12.

1.4 Contact Details

SOC
Telephone number 01908-658100
Email SOC@Securitas.uk.com
Opening times 24/7/365

Admin
Telephone number 01908-658158
Email Arc.admin@Securitas.uk.com
Opening times 08:00 to 17:00 Monday to Friday

Technical Helpdesk
Telephone number 08081686486
Email Technical.Servicedesk@securitas.uk.com
Opening times 24/7/365

2. Technical Infrastructure

2.1 Monitoring Structure, Disaster Recovery and Business Continuity

Through significant investment, our SOCs are supported via a redundant network to which enhanced alarm and voice call routing is managed. To best optimise service delivery, Companies are normally supported by a 'host' centre within our group. However, we may provide services from an alternate centre to maintain customer service levels.

2.2 Telecommunications (voice and data)

The majority of the telephone lines into the SOC are covered by British Telecom's total care maintenance package. On suspecting, or receiving a message form a client, that a line is faulty the Duty Supervisor shall check the line by either dialling into or out from the line.

The telephone systems at Cobra House and the Fenny Stratford SOC are all interconnected in a way that provides a great deal of resilience. In the event one of the systems fails, the handsets shall automatically connect to an alternate phone system. In the event an issue prevents the phones connecting to an alternate system, a software based phone installed on each operator terminal can be configured to connect to any of three specified phone systems.

Calls into the SOC are normally routed through the Fenny Stratford SOC and to the Cobra House SOC. In the event an interruption of service prevents calls being delivered in the normal way, the Supervisor can invoke a call forwarding plan to divert calls to SIP trunk lines presented at the SOC. Instructions how to achieve this shall be stored in the SOC Go-bag. A mobile phone shall be stored in the SOC GO-bag to help making calls in the event of a catastrophic failure. If the supervisor is satisfied that the line is out of order he should report it to British Telecom's fault line and obtain a reference number and log the incident in the Non-conformance Log. The Supervisor may also seek advice from the Duty CTO technician(s).

Should both lines of any receiver group the SOC Director and/or the CTO Director of Technology should immediately be advised. It should be noted that this is likely to be exceptional since signalling receivers are split between Cobra House and Fenny Stratford SOC and connected to independent telephone exchanges. Digital communicator numbers are presented on ISDN lines terminated on server based receivers. Support details for the receivers can be found in the SOC Go-bag. However, any suspected fault should be immediately escalated to the Duty CTO technician(s).

All telephone calls are recorded as required by BS EN 50518.

2.3 Monitoring Product Approval

In the event a supplier wishes to bring a new product to the monitoring market, we have a multiple staged approval process to ensure the product is compatible with our monitoring network and that we have configured response plans to interpret alarm signals received.

Companies using equipment connected to our SOC's that have not been approved do so at their own risk. The full list of currently approved monitoring products is detailed in our monitoring application forms.

3. SOC Administration

3.1 SOC Administration Department

Our SOC administration is provided by a dedicated centralised team. In emergencies, our operational centres can support basic administrative functions but we ask that wherever possible these are requested during normal office hours only (Mon–Fri 08.30 – 17.00).

3.2 Data Security (Passwords)

All SOC's operate a security discipline that requires persons contacting the SOC by telephone to have a valid password before security information can be exchanged.

An audit of engineer's and customer authorised access provision should be completed by the Company at least once per annum. If a customer or engineer is no longer an employee of the Company or End User Site, the SOC should be notified immediately so their access can be terminated from the SOC monitoring system.

3.3 Standard Forms

Due to the security nature of instructions and to provide consistency and minimise errors it is preferred that all applications for monitoring, subsequent data changes and cancellations are completed on the correct form and submitted electronically via email.

We aim to process all instructions received before 12 noon on a weekday during the same working day and instructions received after 12 noon, at weekends or bank holidays, the next working day, (our normal working day is 0800 - 1700 Mon to Fri excluding English Bank Holidays).

3.4 New Connections

All new connections should be processed on our connection forms and be emailed to Arc.admin@securitas.uk.com

3.5 Transferring Systems to our SOC

3.5.1 Single Transfer-in

Ensure that the SOC is in receipt of a completed connection form and the form indicates this is a transfer from another SOC and includes the identification number and the name of the

relinquishing SOC. The application must include details of keyholders, zone requirements and URN's as these are sometimes not provided by the losing SOC.

Once the service provider has received the losing SOC's confirmation, the transfer can go ahead. Our SOC will then inform you that the system is ready and an engineer may be required to attend site and complete the transfer.
If attending site the engineer should contact the SOC.

The engineer should ensure:

- The system is put on test and they advise us they are transferring the monitoring service from another SOC to us.
- Every channel is activated noting order of transmission, i.e. Intruder, Open, Close, Restore, etc.
- The requirements of Section 4.0, Commissioning Approved Products, are followed.
- We have received the correct channels in the appropriate order and have all the correct data, e.g. Contacts/Keyholders, etc.

The system will normally be made 'LIVE' following expiry of the initial test period unless we are instructed otherwise by the engineer.

3.5.2 Volume Transfer-in

The Company is required to provide full details of each connection to be transferred in, including:

- Site Names & Addresses
- Contact Details
- URN's and their status
- Zone Details & Response Plans
- Open/Close Details & Schedules where required
- STU Numbers

SOC Administration will add the details to the Monitoring System Database.
Once agreement is reached that all system details are correct a date of transfer can be agreed between the Company, the monitoring service provider and both SOC's.

SOC Administration on the day of transfer and following days as required will run event history reports to ensure that the systems transferred are signalling correctly or alternatively any specific commissioning requirements agreed with the Company are carried out.

3.6 Takeover of another Company's Monitored Connection at our SOC

It is imperative that the following procedures are adhered to at all times.
1. Both companies involved with the takeover must write to the SOC stating their intention to either release or to accept the end-user to their account. Note: without these documents the SOC will not be able to transfer the site as it is contracted to the current Company. Companies can use the standard application forms.

2. The documents should include the following information:

CS number
Name
Full address
Signalling type
Police Force
URN
URN Status (i.e. Withdrawn or Normal)
Contacts/Keyholders
Zones and alarm response
Proposed transfer date
3. All critical data should be reviewed with the end-user to ensure accuracy.

4. The Company should check the SOC responses are correct and will meet the end-user expectation, attention should be given to pre and post ACPO 2000 responses.

5. Transfers should be carried out Monday to Friday 09-00hrs to 16-00hrs, excluding all bank holidays.

6. Billing will continue up to the transfer date and the out-going Company will be responsible for these charges. After the transfer the new company will be responsible for any transfer costs and the on-going monitoring charges.

7. The URN belongs to the Maintenance Company and the gaining company must write to the authority, (using Appendix "F" of the Police Force Policy), prior to the transfer informing them of the transfer. This may include a fee dependant on the authority. Failure to notify the authority prior to the transfer may render the URN null and void.

8. When the transfer is complete the SOC will normally confirm the cancellation to the outgoing company and a new connection to the new company.

9. It is strongly recommended the system is re-commissioned and fully tested to our SOC as detailed in section 4.2.

10. In the event the out-going company will not release an end-user account to a new provider the only option is for the new provider to apply for a new account in the normal way.

11. The SOC will not accept any responsibility if these procedures are not adhered to in full.

3.7 Alarm Configuration

To establish a common approach across the SOC, the default communication channel designations are detailed in the commissioning section.
Our connection form details the connection type which will normally default by system type to these zones with the appropriate agreed business response. If you wish to deviate from these standard responses this must be clearly indicated on your application or through a pre-existing agreement of default responses.

Changing grade of monitoring products
In the event the monitoring service is re-graded it is essential that the following guidelines are adhered to:

1. The customer should be notified and the alarm system specification updated.
2. It is recommended that the customer is advised to obtain agreement from their insurance company of the grade change.
3. When transferring the data from the old product to the new product a full commissioning test should be carried out, see section 4.2.
4. On completion of the grade change a cancellation of the unwanted product should be completed, refer to Section 3.12.

The SOC does not accept any liability for changes in monitoring product, unless items one; two and three above are completed in full.

Pre-ACPO 2000
Should an existing system be transferred to us and a pre-ACPO 2000 alarm response is to be retained, we must be clearly instructed of this requirement on the application form.

Channel Configuration for EN50131 Systems
Under EN50131 there are requirements to send additional signals such as AC Mains Fail and Tamper faults to the SOC. The main additional requirements are dependent on System Grade as follows:

- For Grade 3 and Grade 4 systems, it is necessary to send AC mains fail signals if the standby battery capacity is to be halved from 24 hours to 12 hours
- For Grade 3 and Grade 4 systems, it is necessary to send tamper signals to the SOC in the set and unset conditions

3.8 Critical Data Omissions (CDO)

In the event that any critical information is missing on completion of a connection, (e.g. Contacts/Keyholders, telephone numbers, URN's, etc.), the Company will be informed of missing information, usually by e-mail, a report will be also sent monthly detailing any missing information on the company estate.

Failure to run or act upon reports received and make corrective actions could result in customers/end-users not receiving the correct alarm dispatch, information they have paid for or incurring additional cost. Our SOC will not accept any liability for failed alarm dispatch or telecommunications costs from a third party supplier or customers/end-users where reports have not been addressed with appropriate corrective actions.

3.9 Data Changes

3.9.1 Securitas Processed Changes
All data changes should be completed preferably via MASWeb or e-mailed to Arc.admin@securitas.uk.com. We aim to process all data change requests received before 1200 hours on a normal working day the same day. All written data changes received after 1200 hours or outside the normal working day will be processed during the next normal working day. The normal working day is defined as: 0830 - 1700, Monday to Friday excluding 'English' bank holidays.

3.9.3 Contacts/Keyholders:

All change requests should list 'all Contacts/Keyholders', this will enable us to check that we have them listed in the correct sequence and update our records accordingly. For changes made via MASWeb it is important that all Contacts/Keyholders on the database have a sequence number and contact telephone number, Contacts/Keyholders with no sequence or telephone numbers will not be presented to a SOC operator for alarm dispatch.

It is important when advising the SOC of new or changes to existing Police and Fire Authority URN's that the elements the URN applies to is specified, i.e.

- PA only
- INTRUDER only
- PA & INTRUDER
- Fire only

Any changes to URN's requested on a weekend are normally processed the next working day.

3.10 Monitoring Suspension & Reinstatement Suspension

A method used by the SOC to ignore all alarm conditions for a period of more than 24 hours. All instructions must be confirmed in writing or via email to arc.admin@securitas.uk.com:

- Billing will continue during the suspension period.
- The SOC will not allow suspensions with an end date.
- The Company must review the suspended systems weekly to ensure the suspension is still required.

Re-instatement

The instruction to reinstate a suspended system is normally required in writing, but may be accepted over the telephone from an Authorised Contact/Keyholder, Company Representative or Engineer.

3.11 Transferring Systems to an alternative SOC

3.11.1 Single Transfer-Out

The SOC's agreement to participate in the transfer of monitored systems to another SOC, unconnected with us, is dependent on the existing contractual arrangements in place between the Company and our SOC. Terms and conditions can apply to both the Company's overall account and to individual monitored systems i.e.

- The account is within an initial fixed term.
- The monitored system is within its first year.
- The agreement to transfer or the agreement to a date of transfer will also be dependent on the payment of any outstanding or future invoices.

Our SOC Administration should be contacted in the first instance to progress any transfer enquiry.

3.11.2 Volume Transfer-Out

1. A written instruction is required from the Company authorising our SOC to exchange information with the alternative SOC.

2. The Company or alternative SOC, on the Company's behalf, shall provide our SOC with a list of systems requiring transfer. Once agreement is reached that all system details are correct a date of transfer can be agreed between the Service Provider and both SOC's.

3. Our SOC will normally cancel the monitoring connections, subject to transfers, within 48 working hours of the agreed date of transfer without further instruction. All rights and liabilities placed on our SOC shall cease at the time of transfer.

3.12 Cancellation

To ensure the accurate and timely cancellation of monitoring services, requests to cancel will only be accepted by the completion of the appropriate Form, Company Email or Letterhead to the Administration Department by one of the following options.

- Email: Arc.admin@securitas.uk.com (preferred option)
- Post: Securitas Security Services, Cobra House, FAO SOC Administration, Wavendon Business Park, Milton Keynes, MK17 8LX

IMPORTANT:

1. Approved and processed cancellations will normally be confirmed back to the Company in writing (email where available), within 24 hours of receipt. Any cancellations submitted that are not confirmed within stated timescales must be queried as failure may lead to a delay in cancellation.
2. We will not respond to alarm signals received following cancellation and it is important that the communicator at the protected premises is removed or disabled to prevent further signals being transmitted and associated telephone charges being incurred.
3. Any cancellations requested on a weekend will be processed the next working day.

3.13 Confirmation of Administrative Instructions

Automatic confirmation is provided by email, or post if not available, for all requests placed for new services and cancellation of existing services; changes to existing services may also be notified by email if required. Should the Company not receive the expected confirmation they should contact the SOC administration team at their earliest opportunity.

It is the Company's responsibility to ensure that instructions sent have been received, this may be achieved by receipt of an automated notice of confirmation for new orders and cancellations.

3.14 Reports

Business Critical Daily / Weekly Reports
Our SOC provides the following reports. It is strongly recommended that all these reports should be run daily / weekly and corrective actions completed on a daily / weekly basis.

1. Daily Activation Reports History – Lists all alarm incidents in the specified date range

2. Weekly Sites not commissioned – Lists sites ordered but not connected out of service category "Needs Commissioning"

3. Weekly Systems in Path Failure – List all sites in signal path failure

4. Daily High Activity Sites – Lists of sites sending excessive signals

5. Daily New Connected Sites Reports – Lists the newly connected sites for the date range specified

6. Daily Systems in Alarm Condition – Lists Unrestored alarm conditions

7. Monthly False Alarm Management – List all alarm conditions that require a reason code

Company Business Critical Monthly Reports

The MASWeb access allows companies to assign disposition codes against alarms and as an aid to compliance with BS 8473 Intruder and hold-up alarm systems – Management of false alarms – Code of practice.

Our SOC encourages the management of false alarms and strongly recommends the use of the specific software written by the SOC to highlight reasons why alarm systems create false alarms and corrective actions to reduce false alarm signal traffic to the SOC.

Automated Reports
The following automated reports are available to the Company on request:
1. Daily Activation Reports History – Lists all alarm incidents in the specified date range

2. Systems in Path Failure – List all sites in signal path failure

3. High Activity Sites – Lists of sites sending excessive alarm signals
4. Health Check Report – this includes:

- Systems Awaiting Connection
- New Systems within the last 12 months
- Suspended Systems
- Systems Cancelled within the last 12 months
- Systems with No Site Password or Common Key-Holder Password
- Systems with less than 2 Key-Holders
- Systems Missing Data such as Premises Phone or Postcode
- Systems without an Agency or URN
- Systems with Reduced Police Response
- Systems with No Scheduled or Log-Only Open/Close within the last 30 days
- Systems with Unrestored Zones
- Systems with greater than 5 activations within the last 12 months
- Systems Out of Service
- Fire System with No Fire Brigade Response

5. Service Call Report (out of hours engineer call handling)

Where there is a requirement to send reports by post these will be sent by second-class post.

4. Commissioning Approved Monitoring Connections

4.1 Monitoring Products

Our SOC's support all major suppliers and their associated products in the security industry. Any new products go through our product approval process, referred to in section 2.3, before being connected to our SOC network.
Every new connection and system upgrade should always be commissioned to our SOC network as detailed below.

4.2 Commissioning procedure

The following procedure must be adopted for all new, transferred and system upgrades.

1. Submit an approved application form to SOC Administration at least 24hrs in advance.

2. Ensure the Commissioning procedure can be completed during normal working hours and before 16:00 hours.

3. Contact our Administration Help Desk on 01908658158

4. Confirm what services are being connected and request the system to be placed 'in-service' & 'on-test'.

5. Test each alarm & restore condition, including single and dual path failures.

6. Check all the SOC responses meet with the end-users expectations.

7. Panel manufacturers and signalling providers may delay certain types of alarm conditions to the SOC so be aware of these delays and how they can be tested.

8. Contact our Administration Help Desk on 01908658158 for test results.

9. Confirm all alarm signals sent have been received in the correct order.

10. The Help Desk will validate the 'Signalling Test' and ensure that all the information required to support the Alarm Response has been provided.

11. On completion, the site will be taken off test and a commissioning report submitted to the Company. It is important that the Company advises the SOC if a Commissioning Report is not received.

4.3 Commissioning Certification

To help the Company identify the standard to which the alarm system is commissioned to the SOC, two critical elements for effective monitoring are assessed during the commissioning process:

1. Signalling – All zones and path failures including dual path failures have been tested and the engineer has called back after the test to validate the results.
2. Data - All Critical Data is present on the monitoring system (MAS), for example

Name
Address & Post Code
Premises Tel Number
Keyholders (minimum of two) with appropriate contact numbers
Password for authentication of false alarms & other enquiries

5. Alarm Monitoring Responses

5.1 Alarm Response Performance

Our SOC's undertake to meet the standards for contacting the emergency services as set out in BS EN 50518 & BS 8591 for Category II SOC's, which are:

1. Fire 30 seconds for 90% of signals received, 90 seconds for 98.5% and 180 seconds for 100%
2. PA 30 seconds for 80% & 60 seconds for 98.5% signals received
3. Intruder 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received.

These targets are exclusive of any imposed filtering period and exceptional circumstances such as extreme weather conditions and the associated abort signals received under these conditions.

5.2 General Requirements – Alarm Signal Processing

Our standard response to alarm signals is detailed within this section. All actions taken by the SOC are as indicated unless the Company advises otherwise. It is the responsibility of the Company to advise the End User what action the SOC will normally follow on receipt of an alarm signal.

All alarms are assigned a priority as indicated in the table below. In the event of multiple alarm signals only the highest priority alarm will be processed.

Signal Type	Priority
Loneworker	9
Fire	10
PA	20
Confirmed Intruder	39
Intruder	40
Line Fault	45
Trouble	46
Environmental	50

Our SOCs will only act on alarm signals received at the SOC. We accept no liability for signals lost for whatever reason by suppliers or their agents.

5.3 Fire and Police (Agencies) Attendance

Agencies may have individual policies which you must comply with to ensure we can dispatch alarms to them on your behalf. The SOC has dedicated telephone numbers with most agencies where appropriate.

Agencies will respond in accordance with their published policies and where they require a URN, it is the responsibility of the Company to ensure the SOC is in possession of a valid URN and its response status is 'active'.
Our SOC will not be liable for delays in response from agencies.

It should be noted that within any contractual agreement or communication we cannot make any commitment that would involve assuming the powers of a civil authority, i.e. UK Police, Garda Siochana or Fire Service, etc.
In some cases agencies may request the Company or the SOC to deviate from normal policy. In these circumstances requests should be made in writing from the agency and directed to the Customer Service Manager or the National Administration Manager. On receipt we will propose a solution and communicate with the company. Such variations should be kept to an absolute minimum. The SOC does not accept any liability for procedures that deviate from standard policy.
Current policies can be accessed from the following web sites. Note these may have regional variances.
ACPO policy (England and Wales) - http://www.acpo.police.uk/
England, Wales and Northern Ireland Police Response to Security Systems
Police Scotland - http://www.scotland.police.uk/
Scotland Security Systems Police Policy
CFOA policy - http://www.cfoa.org.uk
Fire Authorities Policy

5.4 Filtering Policy

The following filtering techniques are in accordance with ACPO Policy, Police Scotland Policy, BS8243 and BS EN 50518.
For alarm systems installed in Southern Ireland the filtering requirements of 'Monitoring Centres for Intruder Alarm Systems' (IS228) and the Garda Siochana Policy on Monitored Intruder Alarms apply.

5.5 Mis-Operation Signals

All systems shall either:

1. Send an unset/set (open/close) signal (Preferred Option)

or

2. Be capable of generating a secondary signal to indicate that the alarm system has been mis-operated.

Where we are unable to identify whether the system is set/unset (open/closed) we will action as "closed".

All intruder alarm conditions are delayed in accordance with the relevant agency policy waiting for a mis-operation signal to abort the alarm. These are:

1. Open
2. Abort

At any time prior to operator intervention if the SOC receives items 1 or 2 the alarm condition will be automatically aborted due to mis-operation.

Open/Close with monitored line communications

Where the SOC is asked to monitor communication path failures, i.e. PSTN/GPRS/GSM/IP Networks & others it is imperative that the transmission equipment is programmed to send open/close signalling to the SOC without exception. The reason for open/close is to allow the SOC to make decisions based on the status of the alarm system to conform to ACPO and EN50131. Failure to enable open/close signalling may render an incorrect response to alarm conditions received at the SOC.

Should a Fire Authority response be required to fire alarm signals this must be specified on the monitoring application form.

Fire Authority responses may be subject to individual Fire Authority filtering policies as per the Chief Fire Officers Authority (CFOA) http://www.cfoa.org.uk .

It may be necessary to contact the premises prior to contact with the Fire Authority. If you have dispensation for the SOC not to call the premises, we will normally need a copy of the letter of authority from the Fire Brigade for the SOC to remove this facility.

Some Fire Authorities require Unique Reference Numbers (URN's) for the SOC to be able to dispatch calls to them. Some Fire Authorities adopting the CFOA call challenge procedures

may refuse to attend a Fire Alarm unless the customer/premises confirms they have a fire & furthermore these Brigades do not accept a 'no reply' as a confirmed situation.

In cases where open and close is monitored via the security system, we will normally not call the premises in response to a fire alarm when they are known to be closed.

If our response to fire alarm signals requires changing we would normally expect to receive this instruction in writing.

5.6 Personal Attack/Hold-up Alarm Conditions

It is our SOC policy that all PA's/Hold Up Alarm conditions are police-able immediately (no filter) with a valid police URN on level one police response. Normal Police rules apply see section 5.3.

Confirmed hold-up alarms
BS 8243: 2010 sets out the requirements for confirmation of hold-up alarms where this is required under ACPO or Police Scotland policies:

ACPO: 2014 states,
"3.4.5 For restoration of HUAs which have lost response, confirmation is mandatory"
Thereby Hold-up Alarm Systems (HAS) will be required to incorporate alarm confirmation technology to gain reinstatement of Police response should the PA URN become withdrawn.
Types of confirmation
BS8243: 2010 clause 4.2.2 states:
"HASs should incorporate one or a combination of the following alarm confirmation technologies:
1 audio confirmation
2 visual confirmation
3 sequential confirmation
4 telephone confirmation (call back)

An explanation of the selected combinations should be provided to the user/client to ensure the most appropriate confirmation technology is used.
Unless agreed with the client in writing, sequential confirmation should be used only in conjunction with telephone confirmation.
The installer should obtain written confirmation of the client/user's acceptance of the chosen option, and detail how the confirmation works".
1) Audio Confirmation

It must be clearly stated on the monitoring application form that audio confirmation is required of Hold-up Alarms and the type of confirmation used. We only accept audio systems with ring back.
Before commissioning the system please ensure the SOC is in receipt of a completed application form and the form states the type of audio verification system used and the telephone number which is to be used to dial up the system for alarm verification purposes.

2) Visual Confirmation
Where visual confirmation is required of Hold-up Alarms for systems designed to comply with BS5979 and BS8243 rather than BS8418.
A typical response to a video confirmed hold-up alarms system is stated below.

2.1 Event is received and upon dialling into the video system there is no sign of activity on site the SOC will contact the contacts/keyholders as an unconfirmed alarm.
2.2 Event is received and upon dialling into the video system there is sign of activity on site the SOC will contact the police and contacts/keyholders.

3) Sequential & Telephone Confirmation
For hold-up alarm conditions to be considered sequentially confirmed BS8243: 2010, clause 5.4.1.2 states:
a) the HAS should be configured so that at least two separate alarm conditions are reported within the confirmation time; and
b) signals emanating from HDs (hold-up devices) should be from either;
1) two or more HDs separately identifiable at the CIE; or
2) a multi action HD.

The hold-up confirmation time should be not less than 8 hours and not more than 20 hours".
It must be stated on the monitoring application form that sequential confirmation is required of Hold-up Alarms and the transmission protocol used.

Before commissioning the system please ensure the SOC is in receipt of a completed application form and the form states the type of sequential verification used and the alarm response required.

Default SOC Response

A) Hold–up alarms system without confirmation will result in only the police being called.

B) Hold-up alarm system with sequential confirmation will result in only the contacts being called for the first alarm and only the police if the confirmation has been received.

The hold-up confirmation time configured by the alarm system control and indicating equipment (CIE) at the protected premises must not be less than 8 hours and not more than 20 hours. If at the expiry of the confirmation time HDs remain in an alarm condition and are inhibited a signal should be sent from the CIE to the SOC.
Notes: 1. To function correctly and to minimise the likelihood of false alarms occurring a signal must be sent to monitoring centre when channels are restored to their quiescent state.
2. For systems sending SIA Protocol: If receipt of the 'HA' mnemonic should be interpreted as
'Duress' and passed to the Police, you must advise us of this on application otherwise it will be interpreted as an unconfirmed hold-up alarm.

To distinguish between a confirmed intruder alarm and a confirmed hold-up alarm for systems signalling both events via the same alarm channel, i.e. usually channel 7 for 'fast format', an extra event is attached to the system called 'CONFPA', this recognises, through interrogation of the previous alarm events, when the alarm should be processed as a confirmed hold-up event rather than a confirmed intruder event.

System Designation
As of 1st June 2012, new systems that specify confirmation of hold-up alarms will attract an alarm response to the requirements of BS8243: 2010 and PD6662: 2010 unless we are instructed otherwise.

If confirmation of hold-up alarms is not specified, our default response plan, will be applied and unconfirmed hold-up alarms will be passed to the police.

It is important to ensure that we are informed of new systems that should receive an alarm response to an earlier standard than BS8243: 2010 and PD6662: 2010 and of existing systems that are upgraded to current standards and should have their response plan changed.

5.7 Intruder Alarms

Type of Alarm	Actions taken by the SOC
Unconfirmed Intruder Alarm	Premises and Contacts/keyholders
Confirmed alarm when closed	Police and Contacts/keyholder
Confirmed alarm when open	Premises or Contacts/keyholders
Unconfirmed alarm followed by an open/abort	No Action Taken

Confirmed alarm followed by an open/abort signal	No Action Taken

All police calling systems must have a unique reference number (URN) for the SOC to be able to dispatch to them.

All new intruder alarm systems installed within an ACPO or Police Scotland Authority Area that require 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 sequential confirmed intruder alarm systems within premises residing in ACPO or Police Scotland Authority Areas are held for 120 seconds in order that they may be aborted or confirmed by a second detector.
Southern Ireland Only: All intruder alarm signals received from sequential confirmed intruder alarm systems within the Garda Siochana Police Authority Areas are held for 60 seconds in order that they may be aborted or confirmed by a second detector.

5.8 Types of Confirmed Intruder Alarm

5.8.1 Sequentially Confirmed Alarms
Sequential alarms are perhaps one of the simplest confirmation technologies. The SOC just needs to know that two independent detectors or two detectors of different technologies have activated within the protected premises.

Signals are held for an intentional delay of 120 seconds for premises residing within ACPO or Police Scotland Authority Area's in order that they may be aborted or confirmed by a second detector.

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 mis-operation signal or a signal to indicate the system is unset prior to any action by the SOC the alarm will normally be automatically aborted.

It is important that 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 SOC from carrying out the incorrect action on any subsequent activation. Should the zone that generated the initial

unconfirmed alarm be isolated on re-arm then a signal should be sent to the SOC to indicate a zone has been omitted.

Southern Ireland Only

Signals are held for a minimum of 60 seconds for premises residing within the Garda Siochana Police Authority Area's in order that they may be aborted or confirmed by a second detector.

Type of Sequentially Confirmed Alarm

A confirmed signal must be delivered by the appropriate mnemonic code within the protocol used, the SOC will not accept 'any' second event as a confirmed alarm condition and for second zone reporting the channels for the unconfirmed and confirmed intruder signal must be pre-designated on application to the SOC.

Open & Close signals with Point ID and SIA

It is strongly recommended that open/close signals are enabled to the SOC when using Point ID and SIA. In the event the Company wishes to disable open/close thorough checks must be made by the Company to ensure all associated signals are also disabled when commissioning the site.

It is the Company's responsibility to ensure that every element of the connection is tested with the SOC and the response required is confirmed.

It is imperative when changing control panel suppliers that a full test is carried out with the SOC to ensure the connectivity and response required is correct.

The SOC cannot accept any responsibility for Point ID and SIA systems where the open/close signals are disabled and associated zones are left enabled with no additional zones being created.

5.8.2 **Audibly Confirmed Alarms**

Audio confirmation requires the SOC to listen to audio data from the protected premises following the receipt of unconfirmed intruder alarm signals. We only accept audio systems with ring back.

Before attending site please ensure that SOC is in receipt of a completed Connection Form and the form states the type of audio verification system used and the telephone number which is to be used to dial up the system for alarm verification purposes.

The SOC should be contacted prior to the system being connected to place the system in-service and on-test.
Testing of all microphones should be carried out in local mode by the engineer on site in accordance with the manufacturers' recommendations.

When you are satisfied with the audio coverage, the SOC should be contacted to carry out a test dial into the site to ensure the system is working correctly and sounds can be heard.

For compliance with BS8243, audio systems must incorporate technology capable of detecting and signalling to the SOC a sequential confirmation alarm should two detectors activate that meet the sequential confirmed requirements of this code of practice.

Should a sound be heard then we will treat as a confirmed alarm. The SOC will not use discretion.

The maximum time our SOC agent should listen is one minute. The Company must ensure audio systems are configured to provide this response to ensure the alarm receives the correct action by the SOC. All audio systems must send open/close signals to the SOC

5.8.3 Visually Confirmed Systems
We provide CCTV monitoring through our CCTV monitoring platform Immix.

For systems designed to comply with BS5979 and BS8243 rather than BS8418: Video systems must incorporate technology capable of detecting and signalling to the SOC a sequential confirmation alarm should two detectors activate that meet the sequential confirmed requirements of BS8243.

5.9 Path Failure Alarm Conditions
EN50131 and EN50136 calls for signalling suppliers to report line failures to the SOC in the following timings

Grade	Primary	Secondary
Grade 2	25 Hours	25 Hours
Grade 3	5 Hours	25 Hours
Grade 4	180 Seconds	5 Hours

Signalling supplier's interpretation of this standard may be different depending on grade and supplier. Please check with your nominated supplier for the reporting times by grade.

The SOC will only respond to path failures received by the monitoring software (MAS) as documented below unless otherwise instructed by the company or end-user or the site has become troublesome as detailed in section 5.15. Changes to response must be documented in writing.

Alarm Type	Status	Response
Single Path Failure	Open	Notification Via Email
Dual Path Failure	Open	Premises or Contacts
Single Path Failure	Closed	Notification Via Email
Dual Path Failure	Closed	Premises or Contacts

3. Systems that monitor path failures must also transmit open/close signals and restores without exception to the SOC. This is to ensure the correct response to path failures is carried out. Care should be taken to ensure the open/close signals are working the correct way round. Our SOC will accept no liability for incorrect actions where the open/close signals are working back to front.

4. The SOC may abort a response if the line failure restores in a reasonable time frame.

5. On receipt of restore signals the status of the corresponding path failure condition will be returned to its dormant state, the SOC will log this event.

6. STU's that have temporarily lost power due to power supply problems may go into 'no-response'. The use of the "UP STU" command also allows for the possibility of STU substitution in an attempt to compromise the system. Our SOC recommends that the "UP STU" command is only used on instruction from an alarm engineer who has previously placed the systems "on test" from the customer's premises. Our SOC will only "UP" a STU in response to an alarm event with a valid password or with prior written authorisation from the Company and we do not accept liability for any loss or error that may occur as a result of this action.

7. Single path failure conditions of EN50131 Grade 2 & 3 systems are normally filtered for 60 minutes and Grade 4 systems for 2 minutes in order that the alarm may be aborted through receipt of a restore signal to avoid unnecessary call to Keyholders.

All intruder alarm signals received from sequential confirmed intruder alarm systems within premises residing in ACPO or Police Scotland Authority Areas are held for 120 seconds in order that they may be aborted or confirmed by a second detector.

Southern Ireland Only
Where the alarm signalling and monitoring arrangements are such that a communication or transmission fault might possibly give rise to Garda Siochana call-out, the Company should advise the subscriber in writing at the time the alarm-monitoring agreement is being set up that communication or transmission faults that result in Garda Siochana call-out can adversely affect future Garda Siochana response to the alarm system.

Path Failure Reporting
Our SOC will normally advise the Company the next working day by report should a Path Failure remain in 'Fault' for greater than 24 hours. Systems set to ‘log only’ may not report. Our SOC considers that any 'duty of care' responsibilities to the Company in respect to systems exhibiting signal failure will have been fulfilled following the above actions.

5.10 Fault and Other Advisory Alarm Conditions
Following the increased signalling requirements of EN50131 the number of signals to be sent to the SOC have noticeably increased, especially those categorised as low priority or advisory.

Customers recognise these low level alarms as ‘advisory events’ and in many cases, dependent upon their circumstances, only require that these are recorded in a report for subsequent review.

The default response to a range of fault and advisory events will be for our IVR system to automatically call the premises and/or contacts/keyholders. If the signal restores in an acceptable amount of time then the alarm will be aborted.

All these events are available by report for the Company to view the next working day as necessary. It is the Company’s responsibility to action these events to the end-user where applicable and to ensure corrective actions are carried out as required where required.

Where the event is a trouble, polling, communications path or other unexpected event, it is recommended that a full test of the alarm system including every zone and all signalling paths is carried out to the SOC for each alarm and restore channel.

All events are available as LOG only where requested by the customer.

5.11 Linkdown Message

"Linkdown" is a message sent to the SOC if the BT Scanner in the exchange has lost connectivity with the subscriber transmission device (STU) normally through planned outages on the BT RedCARE network. Our operational teams suspend these "Link Down" messages normally from 60 to 120 minutes depending on the severity of the volume of alarms as the majority do restore (Link OK) in this time. This could in some circumstances effect the transmission of the GSM also.

As a duty of care if we do not see the "Link OK" in a reasonable time frame we will notify the customer of the situation.

5.12 Late Restoral Alarm

BS8243 requires all intruder signalling systems to send restores without exception. All connections should be commissioned with the zones working the correct way round. It is bad practice to ask the SOC to invert the response and act on restores.

The majority of intruder and path failure conditions that have failed to restore in approximately 90 minutes from full clearing the alarm condition may be reported by the LRAC processing. The Late Restoral Alarm processing is a reportable service on MASWeb.

When the Company identifies a Late Restoral Alarm, they should proceed to restore the alarm condition as soon as possible.
Where the Late Restoral Alarm is a signal path failure this may take longer to rectify by the path supplier but still needs the company's attention. Until the alarm zone is restored, the SOC may not be in a position to action any further alarm conditions from that zone or zones, this includes signal path failure alarms.

5.13 Systems with Opening and Closing Time Schedules

Our SOC offers timed monitoring for open and close signals against a time schedule normally at an additional cost.

LTC – Late to Close (Additional charges may apply)
ETO – Early to Open (Additional charges may apply)

Late to Close and early to open notifications
Response to the above notifications would normally be from our operators, when calling the premises they will request a password and a new close time, this new close time will be added to our system.

This process should be repeated if the protected premises has not closed by the new close time. If the premises do not answer or confirm the correct password the call will be referred to premises keyholders. If there is no response from any keyholder we will try for a maximum of 4 hours after this the alarm will be cleared from our system.

5.14 Digital Communicator – Timer Tests

Systems communicating via Digital Communicators that are required to send a signal to the SOC every 24 hours which meets the requirements of EN50131, should be configured to send daily timer test signals. The SOC monitoring system will normally log these signals and should a Digital Communicator fail to signal, the Company will receive an automated email at the time of the missed signal.

5.15 Unknown Signals

If the SOC receives signals from a site/customer but the signal is unknown to the SOC we will normally disregard the signal. This unknown signal will be reported to the customer the next day on their daily report.

5.16 Excessive Signals

The SOC monitors excessive signal traffic. Should a particular site/system become 'troublesome', through the receipt at the SOC of unknown signals, unwanted signals or repetitive alarm incidents, we will normally inform the company of the site affected. Our SOC reserves the right to charge for excessive signal traffic.

5.17 Calling Contacts/Keyholders

There should be a minimum of two Contacts/Keyholders available 24 hours a day for seven days per week, unless a 24-hour key holding service is utilised in accordance with ACPO requirements. It is recommended, even if a 24-hour key holding company is employed, that key holders are still maintained in the unlikely event the key holding company are unable to attend.

When calling the contacts/keyholders we will ring for approximately 60 seconds before terminating the call, if the contact/keyholders are unavailable at the time of the alarm we will sleep the alarm for a minimum of 15 minutes and will make further attempts to contact them up to but not exceeding 2 hours.

When the SOC initiates the telephone call to the Contact/Keyholder we normally ask for the named contact but we don’t require a password at this point. Once a legitimate Contact/Keyholder has been contacted the incident will be closed. Should a Contact/Keyholder decline to attend the premises it will be their responsibility to contact

another authorised Contact/Keyholder. The SOC cannot advise on what actions the Contact/Keyholder should make. It is recommended if the SOC calls a Contact/Keyholder they attend the protected premises without exception.

Interactive Voice Response (IVR)

We currently use an IVR to deal with low priority alarm events, the IVR system will call the contact/keyholders and notify them of the full address of the site and the alarms that has been received. The recipient of the IVR call will need to press 8 on their telephone keypad to accept the call. In the event that the recipient does not answer or does not press 8 the system will call the next contact/keyholder on the list. In the event all contacts/keyholders have been called and none of them accept the alarm, the system will sleep the alarm and try again after 5 minutes.

5.18 Calling Premises

There are two premises telephone number fields available on the monitoring database and only premises telephone numbers should be contained in these fields. Under no circumstances should the premises number be inserted in the keyholder fields as this may cause confusion for operators and may render the password not being requested which is a security risk.

5.19 Adverse Weather Conditions – Delays in Monitoring

Our SOC maintains operating levels to meet normal fluctuations of alarm signal traffic and have contingency plans in place should alarm signals reach unacceptable levels. In exceptional circumstances, notably through severe weather conditions where signals received exceed the number of operators available, the alarm queue will normally be managed in order of priority by type of event and time of receipt. In such conditions, if an Abort or Open signal is received from a queuing alarm condition this may be aborted and not presented to an Operator.

If the delay continues, only the highest priority alarms may be dispatched. The SOC may introduce automated keyholder contact during this period.

5.20 Multiple Signalling Sites/Systems

It is strongly recommended that for every signalling system only one site is associated. Connecting multiple signalling sites/systems can be very complex in nature and should be discouraged.

For example, a digital communicator signalling with two intruder sites shop 1 and shop 2 should have separate zones/pins per shop.
The commission process would need to ensure that both areas are fully tested.

We accept no liability if sites are not fully commissioned to the SOC.

5.21 Multiple Path Failures (Flood Conditions - WebWay)

All networks are susceptible to disruption and occasionally this may affect a large number of remote locations monitored by the SOC. The potential impact on the operation is serious as multiple communications failures are reported to our agents simultaneously.

Flood condition identifies a mass network outage and protects the SOC from a flood of communication failures being delivered to operators. The end-user should benefit from unnecessary disturbance due to planned/unplanned network maintenance that does not compromise the integrity of their remote IAHS systems (where dual path systems have been deployed).

Activation of Flood automatically delivers a high level alarm to SOC support. The status of the sites affected are then monitored, and once the network outage has cleared Flood Condition is released.

Flood does not block the delivery of alarm activations from the protected premises to the operator (e.g. Fire, Intruder, Open, Close, Confirmed Intruder, etc.).

5.22 Reasonable Alarm Monitoring and Associated Charges

Our SOC reserve the right to charge for additional alarm/activity where excessive traffic is not fair and reasonable and deemed to be over and above normal expected levels, before any charges are received we will attempt to contact the customer and notify them via email. Once the email has been sent the SOC expects the customer to rectify the issue in a reasonable amount of time.

5.23 Pre ACPO Responses

The following is our SOC standard alarm response plan for systems issued with a URN prior to ACPO 2000 or ACPOS 2002 (as amended 1st April 2005), which have not had their police response withdrawn.

Service Type	Response
PA	Police
Intruder (Site Closed)	Police & Contacts/Keyholders
Confirmed Intruder	Police & Contacts/Keyholders

5.24 Remote Resets

On receipt of a telephone request for a remote reset by an end user the operator must

ensure that the guidelines are followed as per British Standards document BS 8473:2006+A1:2008, Section 10.1 to 10.9.
Callers who demand or believe they have a right to Remote Reset will still be fully checked before a remote reset is authorized. If the caller is unable to quote the correct code word then no remote reset will be authorized, the caller will be asked to contact the site Maintenance Company. When a request for a remote reset is received the caller's identity will be confirmed by use of:

The Account Number
The Account or Keyholder code word
The Account Name and Address
The Engineer's ID Number
The caller will then be asked the reason for the activation which must have been received at the SOC. The following are valid reasons for activation/reset when authorized by the Customer or at the request of the alarm engineer:

1. A Keyholder error
2. An incorrect entry procedure;
3. An incorrect exit procedure;
4. Insecure premises;
5. A twenty-four hour circuit has been activated (i.e. a fire door has been opened);
6. An animal or insect has caused the Alarm to activate.
7. The reset has been authorized by the Customer;
8. The reset is at the request of an Alarm Engineer.

A check will then be made on the account history file of our Alarm handling computer. If there are any previous activations on the account for which a valid known reason has been given, but if police action has been taken twice within the last rolling twelve months, the reset may be refused and the caller asked to contact the site maintenance company. If the caller is unable to give a valid known reason the caller will be asked to contact the site maintenance company and the remote reset will be refused. If the Caller can give a valid reason and has not had two polices alarm within a 12 month rolling period then the remote reset will be given by:

1. Log into the remote reset program and find the account.
2. Ask the customer what reset code they have
3. Put this code into the code box and click get reset
4. Give the code which is generated to the customer to enter in his alarm panel
5. If the reset was successful then click on successful reset
6. If the reset was not successful the click on failed remote reset and inform the customer that they need to contact they maintained company to get them to reset the system

6. Placing a System On or Off Test

6.1 Testing Conditions

It is imperative if a system is being tested by a customer/engineer that it is placed 'on test' prior to testing. This will ensure that whilst testing, an alarm conditions are not passed to an SOC operator for action and the creation of a call to the emergency services in error. To place systems on test we have a few options:

1. The use of MASWeb
2. The use of MAS Mobile
3. Call the SOC

All monitored alarm systems must have a unique identifier number known as the chip number and an authorised password.

6.5 On Test Expiry Conditions

All test periods expire automatically at the time set upon the commencement of a test period or earlier if the Engineer/Customer contacts the SOC to complete the test.

If the SOC monitors restore conditions and a test automatically expires, but the system has not been restored and remains in alarm, such conditions will be reported to the customer the following day via their daily reports. The SOC will not accept any liability for tests that expire with unrestored alarm conditions.

7. CCTV Pollution Management

There is a significant differential between healthy, well and regularly maintained sites and those that have not been subject to review of procedures, false alarm activations and servicing schedules on a regular or routine basis. There can be a serious impact from a site that is not healthy, well and regularly maintained and where pollution and false alarm activity is not periodically reviewed with corrective action being taken.

Securitas apply a prioritisation for handling CCTV alarms in a manner that is fairer to customers. The rationale for this is a small number of highly polluting sites may generate a significant number of false alarms, the volume of these alarms impacts on customers whose sites generate a low or expected volume of alarms.

For the purpose of remote CCTV monitoring false alarms are defined as an CCTV alarm that is activated, set off or signals to the monitoring station needlessly; causes an alarm or indicates an event that proves to be unfounded; or gives a warning about untoward activity that fails to be present or happen.

On a 3 monthly basis a review will be undertaken to calculate the average number of CCTV alarms generated by a site on a per month average basis. After this the below grading criteria will be applied. A site where the highest score below has been applied, represents the highest priority in how a CCTV alarm from a site will present to a SOC Operator for handling. The lowest grading will present to the Operator as the last alarm to process. The rationale being that an average or standard site for example, sending an average of 150 CCTV alarms per month will receive a faster response than a site that is sending 10,000 alarms per month.

The grading table below sets out the grading of sites based on (the 3-month average) number of CCTV alarms received:

Priority Grading Highest to Lowest	Monthly CCTV Alarms (3 month average)
500	0-250
400	251-1,000
300	1,001-10,000
200	10,001-25,000
100	25,000+

CCTV Alarm Reporting

Our SOC produce a range of reports of site CCTV activity which are disseminated by email direct to customers. These are available on a daily, weekly, monthly and/or ad-hoc basis. The purpose of the reports is to highlight the activity, functionality and health of a system. I.e. no alarms over a number of days indicates an issue at site which requires urgent investigation, likewise a very high number of alarms (considered to be in excess of 300 per month) indicates a system that requires review and investigation by the owner and/or their engineer to reduce the number of false alarms generated.

Customers are strongly recommended to have a robust process to review alarms on a regular basis and it is recommended that this is combined with CCTV system walk testing and service schedules.

For any support or reporting requirements please contact SOCreporting@securitas.uk.com

Appeal Process

Should a customer take remedial action to resolve the number of false CCTV alarms being signalled through from a site and wish their grading to be reviewed prior to the end of the 3-month review period, to ensure that it is more accurately graded, this can be done by emailing the ARC Administration team requesting in the title of the email 'CCTV Grading Review Appeal'.
The ARC Administration team email address is: Arc.Admin@securitas.uk.com

8. Additional Services

8.1 Out of Hours Emergency Demand Service Calls

Our SOC is able to offer an additional service to the Company for the handling of out of hour's service requests from their clients outside of normal working hours.

- Procedure – On receipt of a call from your customer, we will take their name, address, contact name and number, reference numbers and what their issue is. These details will be entered onto our system, whereby a message will be raise. We shall contact the on call engineer via telephone. If we are unable to contact the engineer we will continue to call them every 15 minutes. After 3 attempts we will proceed to call the companies escalation contacts.

This service is available from 17:00hrs until 08:30hrs weekdays, all weekends and covering all recognised Bank Holidays as standard.

8.2 Lone Worker Monitoring Services

Our Alarm Receiving Centre is inspected and approved for the monitoring of lone worker devices to BS 8484 the code of practice for the provision of lone worker device services by the National Security Inspectorate.
Lone workers are vulnerable from all aspects of risk and the provision of a lone worker device may assist in summoning an emergency responder to assist when incidents occur that requires assistance from a third party.
To enable the SOC to monitor and respond to signals received from a Lone Worker Device effectively the following conditions apply:

1. The Lone Worker Device must comply with the requirements of BS8484 and the supplier must issue a certificate of conformity for the device confirming compliance with and detailing how compliance is achieved.
2. The type and model of lone worker device must have been accepted by the SOC as compatible with its alarm monitoring platform and permit alarm signals to be managed to the requirements of BS8484.
3. The SOC must be in receipt of a Monitoring Application Form for each device providing personal details of the user as defined within BS8484.
4. The SOC may only pass lone worker alarms to the emergency services where listening-in by the SOC operator or whilst in conversion with the user it is deemed by the SOC operator that an emergency response is desirable. In all cases an emergency responder other than the emergency services must be provided to assist the user in cases where an emergency service response is unavailable.

The requirements for Police attendance to lone worker devices is set out within Appendix V of the ACPO Policy.

Incident data, alarm response plans, personal details of lone workers and customer details, as provided to enable effective monitoring and response to activations received from lone worker devices, are held within our BS EN 50518 approved SOCs.

9. Data Protection

9.1 General Data Protection Regulation

We will only process the personal information in accordance with your written instructions. All our staff who process personal information provided by you are under a contractual obligation of confidentiality. Securitas will provide reasonable support to assist you in complying you're your obligations under the GDPR. In the event of a data breach, we will notify you immediately and provide the necessary support to enable you to comply with the requirements of the GDPR and resolve the incident.

Personal information relating to you, your employees, your customers, their authorised contacts and Keyholders will be held by our SOC on the Alarm Monitoring System. Please ensure that relevant names, addresses and contact details are correct. Information received by post or email, including replies and forwarded copies (which may contain alterations) subsequently transmitted from the SOC are confidential and solely for the use of the intended recipient within the purpose of the original transmission. The SOC will retain this data including personal information either electronically or in hardcopy. Telephone calls to and from our SOC's are recorded for security purposes and you must ensure your employees, clients and their authorised Contacts/Keyholders are aware of this. You must ensure that you have a lawful reason to process the personal information you provide to us. Personal data is retained for the periods defined within our Quality System. This is in accordance with our recognition of operating BS EN 50518, as recognised by NSI, for the monitoring of Intruder Alarms and Fire Alarms. Company employees who have access to personal data, alarm system information and activation records are security screened to BS7858 as part of the company induction process and continued employment is dependent on successful security screening.

9.2 Audio Recording for SOC Telephone Conversations

Our SOCs have to comply with BS EN50518, therefore all inbound and outbound telephone conversations are recorded and held for a period in excess of one year. These recordings are the property of our SOCs. We will only release copies of these recordings under the terms of the Data Protection Act.

Release of recording to Data Subjects

By law, we must gain permission from all parties involved in the telephone conversation before we can release copies. It is imperative even if we release copies these are not copied or played back to a third party without our permission. To identify and reduce time taken to recover telephone conversations it is necessary for the exact time and date of the telephone call to be provided, without this information we will be unable to fulfil the request. The copies will only be released by e-mail, and we reserve the right to charge for the service. We do not normally make transcripts of audio conversations.

10. Glossary Term	Definition
Alarm Condition	Condition of an alarm system, or part thereof, that results from the response of the system to the presence of a hazard.
Alarm Filtering	Procedure whereby signalled alarm conditions are intentionally delayed at the SOC and their status reviewed for the purpose of preventing unnecessary calls to the relevant emergency service by cancelling certain alarm conditions in line with industry standards. It is the obligation of the Company to ensure the Customer is aware that some alarm signals may be filtered.
Alarm Message	Message conveyed from an SOC to the relevant emergency service indicating that an alarm condition has occurred at a protected premises, or providing supplementary information concerning a previously reported alarm message.
Alarm Receiving Centre (SOC)	Continuously manned remote centre to which information concerning the status of one or more alarm systems is reported. We trade in the UK under the trading name Securitas UK Ltd.
Alarm Signal	Signal which, upon being received at an SOC or other remote location, identifies a signalled alarm condition.
Alarm Transmission Equipment (ATE)	Defines equipment that transmits signals to the SOC.
Agency or/and Agencies	An emergency service for example Police, Fire, Ambulance, Key holding Service, etc.
Audibly Confirmed	Status in which an incident has been confirmed by an SOC Operator at a remote location (normally an SOC), having interpreted audio information transmitted from the protected premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred.
Confirmed Alarm	Condition that follows after two independent actions or signals have been generated from an audible, visual, or sequential source confirming there is a high probability that a genuine alarm has occurred.
Control and Indicating Equipment (CIE)	Equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information.
Commissioned System	A statement used by the SOC to facilitate the connection process to ensure all the critical data is present and the signalling system has been tested to the SOC and commissioned by the attending engineer.
Company or Companies	Organisation that provides service and maintenance for alarm systems or who pays for

	the monitoring service for example Alarm Company, National Account or End User.
Contact / Keyholder	A representative of the protected premises with authority to make changes to the SOC response to signalled alarm conditions and/or attend the protected premises in response to signalled alarm conditions.
Control Panel Unit (CPU)	The user interface for the alarm system.
Customer / End-user	Person or organisation utilising the services of an Alarm Company.
Disposition Reason	Reason for alarm activity
Early to Open (ETO)	A system that is unset prior to the scheduled opening time
Global System for Mobile Communications (GSM)	A network used by some signalling devices to transport alarm conditions to the SOC.
General Packet Radio Service (GPRS)	A network used by some signalling devices to transport alarm conditions to the SOC.
False Alert (FA)	Signalled alarm condition that without having been extended to the relevant emergency service is regarded by the SOC as cancelled either by an open or abort, if programmed, or mis-operation validated by the customer / end-user quoting their authorised password.
History	A table of event history, including open/close signal, alarm conditions, SOC actions and service call out logs (where applicable).
Hold-up Alarm System (HAS)	An alarm system that incorporates Hold-up/Panic Alarm Devices
Intruder Alarm System (IAS)	An alarm system that is designed to detect intrusion.
In Service	A site/system placed 'in service' has reached a status where alarm conditions received will be processed by the SOC.
Internet Protocol (IP)	A network used by some signalling devices to transport alarm conditions to the SOC.
Local Area Network (LAN)	Local Network available to support communication suppliers to transport alarm conditions to the SOC.
Last Alarm Condition	The last time an alarm condition was communicated to the SOC from the protected premises.
Late Restoral Alarm Condition (LRAC)	An alarm condition that has not restored to its quiescent state within a predefined period.
Late to Close (LTC)	A system that remains unset after the scheduled closing time.
Line Failure/ No Response / Line Fault / Path Failure	A break in the communications link between the protected premises and the SOC.
MasterMind	The Alarm Receiving Centre monitoring software.
Mis-operation signal	Signal that is definitely and unambiguously identifiable at the SOC as indicating to the SOC that the alarm system has mis-operated and

	therefore that the alarm signal is to be filtered out and not extended to the relevant emergency service.
Monitoring Centre Transceiver (MCT)	Alarm transmission equipment.
On test/off test	A mechanism for an authorised person/engineer to ask the SOC to ignore alarm conditions during a period of time not exceeding 24hours.
Operator / Agent	A member of the SOC team who may be involved in dispatch of alarm conditions or administrative procedures.
Order	The result of sending a monitoring application form to the SOC.
Out of hours (OOH)	Out of normal working hours
Out of service (OOS)	Alarm signals received for a site/system that has been placed out of service will be ignored until such time that instructions are received to reinstate the monitoring service.
Personal Attack/Hold Up Alarm	A manually operated device at the protected premises, normally requiring a double input to be activated
Paknet - Vodaphone	A network used by some signalling devices to transport alarm conditions to the SOC.
Polling	A process used to determine if the signalling system is still in place and operational.
Polling Server (PSV)	The server that is polling the communication device.
PIN (Personal Identification number)/ Password	A unique identifier for the customer / end-user / engineer to identify themselves to the SOC.
Protected Premises	The part of a building to which protection is afforded by an alarm system.
Public Switch Telephone Network (PSTN)	A network used by some signalling devices to transport alarm conditions to the SOC.
Receiving Centre Transceiver (RCT)	Alarm transmission equipment.
Remote Restore / Remote Reset (RR)	A process where the customer/end-user calls a Restore Management Centre, normally the SOC, to obtain a code to facilitate resetting of the alarm system.
Response Agreement	Set of instructions agreed between the SOC and the Company or End User as to the actions to be taken in the event of an alarm signal being received by the SOC.
Restore	An alarm condition that has restored to its normal state.
Router	Multilayer switching device
Sequentially Confirmed	Status in which confirmation emanates from two or more independent sensors, detectors, hold-up devices and/or processors, which are so configured that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred.

Signalled Alarm Condition	State of monitoring equipment at an SOC (or other remote location) that indicates intrusion, attempted intrusion or unauthorised interference has occurred at the protected premises, or is likely to occur.
Signalling	The transmission of an alarm condition from the protected premises to a remote location.
Signalling Devices	Transmission equipment for sending alarm conditions to the SOC.
Site/Protected Premises	The location where the alarm is installed.
Status	This identifies the status of a zone and if it requires restoring.
Supervised Premises Transceiver (SPT)	Alarm transmission equipment
Suspend Monitoring	A method to ask the SOC to ignore alarm conditions for more than 24hrs, billing continues during this period.
System	The alarm system installed at the protected premises.
Unconfirmed Alarm	A single alarm activation, i.e. a signal that has not been designated as audibly, visually or sequentially confirmed
Unset / Set or Open / Close or Disarm / Armed	Varying terms used to describe if an Intruder Alarm System (IAS) is set or unset.
URN & URN Status (Permit & Permit Dispatch Status)	The Unique Reference Number (URN) issued by the Police or Fire Authorities and the status, for example Level 1 (On Response) authorities may attend or Level 3 withdrawn (Off response) authorities may not attend.
User	Person authorised to operate an alarm system.
Visually Confirmed	Status which is confirmed by an SOC Operator being at a remote location (normally an SOC), after having interpreted a visual image transmitted from the protected premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred.
Wide Area Network (WAN)	External Network for communication suppliers to transport alarm conditions to the SOC.
Zones (Channels)	Segmentation of the alarm system to enable differing alarm conditions to be identified and signalled to the SOC.

11. Certification

NSI GOLD

CERTIFICATE OF APPROVAL

This certifies that

SECURITAS

(Prop: Securitas Security Services (UK) Ltd)

Cobra House
Ortensia Drive
Wavendon Business Park
Milton Keynes
MK17 8LX

has been assessed and satisfies the requirements of the

NSI ARC GOLD SCHEME

with respect to the following scope:

Monitoring of Fire Alarms,
Monitoring of Intruder & Hold-up Alarms and
Monitoring of CCTV Systems used in Security Applications
in accordance with the requirements of:

BS EN ISO 9001:2008,
NSI SSQS 102, BS 8591:2014,
BS EN 50518:2013 and BS 7858:2012
for services provided
at
ALARM RECEIVING CENTRE – MILTON KEYNES
For
National Security Inspectorate

Chief Executive

18 April 2016	51773	14 September 2018
Effective Date	Certificate Number	Expiry Date

UKAS PRODUCT CERTIFICATION 0142 UKAS MANAGEMENT SYSTEMS 0142

Date Printed 18 Apr 2016

Further clarification regarding the Scope of this Certificate may be obtained from NSI, Sentinel House, 5 Reform Road, Maidenhead SL6 8BY
The use of the UKAS Accreditation Mark indicates accreditation for the scopes detailed on UKAS Accreditation Certificate No. 0142.
National Security Inspectorate (NSI) T 01628 637512

This certificate remains the property of NSI and must be returned on demand.
Approval is conditional upon the Approved Company complying to satisfy all the rules and other requirements applicable to this certification scheme.
National Security Inspectorate is a trading division of Insight Certification Limited. nsi.org.uk

CER009

SECURITAS

Alcumus ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

7th Floor, Russell Square House, 10-12 Russell Square, London, WC1B 5EH

and as detailed on the Annex to this certificate

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 9001: 2008

Certificate Number:	**3360-QMS - 001**
Initial Registration Date:	11 July 2002
Re-issue Date:	18 July 2017
Expiry Date:	15 September 2018

Scope of Registration:

The provision of manned security services including uniformed static guards, guard control systems incorporating a national communications centre, in accordance with the requirements of BS 7499, BS 7858, BS 7984 and BS 7958 Annex C.
The provision of an Alarm receiving Centre, monitoring services and alarm response in accordance with IS 228.

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting Alcumus ISOQAR. This certificate is one of several issued to registration number 3360.

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/isoqar

SECURITAS

Alcumus ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

7th Floor, Russell Square House, 10-12 Russell Square, London, WC1B 5EH

and as detailed on the Annex to this certificate

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 14001: 2004

Certificate Number:	**3360-EMS - 001**
Initial Registration Date:	4 March 2010
Re-issue Date:	18 July 2017
Expiry Date:	15 September 2018

Scope of Registration:

The provision of manned security services including uniformed static guards, guard control systems incorporating a national communications centre, in accordance with the requirements of BS 7499, BS 7858, BS 7984 and BS 7958 Annex C.
The provision of an Alarm receiving Centre, monitoring services and alarm response in accordance with IS 228.

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting Alcumus ISOQAR. This certificate is one of several issued to registration number 3360.

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3899 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/isoqar

CERTIFICATE OF REGISTRATION

Alcumus ISOQAR

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited
Securitas Security Personnel Limited

Securitas House, 271 High Street, Uxbridge, Middlesex, UB8 1LQ

and as detailed on the Annex to this certificate

has been approved by ISOQAR

3360

ISO 27001: 2013

Scope of Activities:

The information security management system covering IT, Support Centre, Alarm Receiving Centre, Human Resources, Payroll and Finance from Securitas locations in Uxbridge, Wellingborough, Milton Keynes and Birmingham in accordance with the Statement of Applicability version 1

Certificate Number:	**3360-ISN - 001**
Initial Registration Date:	**2 March 2015**
Expiry Date:	**2 March 2018**

Signed by:
Steve Stubley, Technical Director
(on behalf of ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting ISOQAR.
This certificate is one of several issued to registration number 3360.

ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester, M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com www.alcumusgroup.com/isoqar

LICENCE
Private Security Services Acts

The Private Security Authority in exercise of its powers under section 22 of the Private Security Services Acts 2004 and 2011 hereby grants to

Securitas Security Services (UK) Limited of Securitas House, Cuckoo Wharf, Lichfield Road, Birmingham B6 7SS. trading as Securitas Security Services (UK) Limited of Securitas House, Cuckoo Wharf, Lichfield Road, Birmingham B6 7SS.

the following categories of licence:
Security Guard (Alarm Monitoring)
Security Guard (CCTV Monitoring)
This licence has been issued by the Private Security Authority on 9 January 2016 and shall expire unless sooner surrendered on 9 January 2018

Licence Number: **04316**

The Private Security Authority
- 9 AUG 2016
An tÚdarás Slándála Príobháidí

Chief Executive Officer

An tÚdarás Slándála Príobháidí
The Private Security Authority

PSA 06576