



Operations Manual

19:30 September 2024

Live Issue

Southern Monitoring Services

Contents:

Foreword & References	2
Contacts	3
Operational Procedures	4-19
Privacy & Legal	21



Foreword

This document detailing our procedures has been produced to help Customers in their day-to-day dealings with SMS.

Please read the procedures contained in this booklet carefully and be sure that all personnel who will have dealings with us understand them fully. This will avoid any misunderstandings and possible delays and enable us to provide a quality service to you and your customers.

This document is the property of Southern Monitoring Services Ltd (SMS) and should not be used, copied, or distributed without our express permission. It is produced exclusively for SMS customer use. It should be read in accordance with our standard terms and conditions.

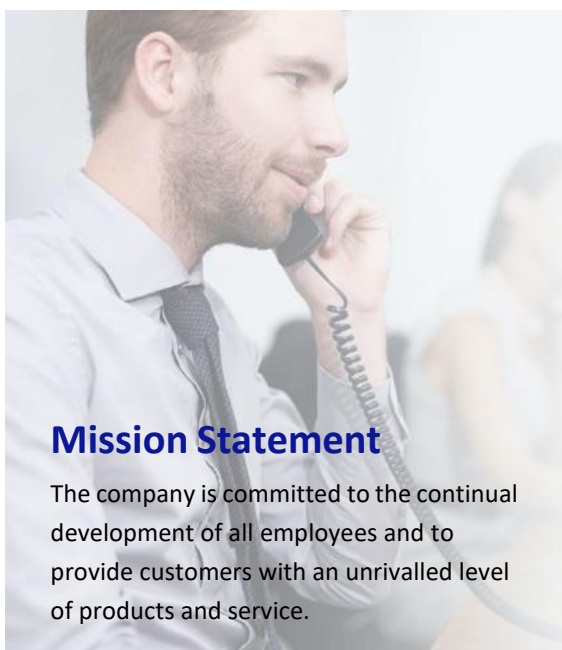
References

This manual has been produced with due reference to Industry Standards and is intended as a guide to alarm companies who utilise our monitoring services.

This manual should be read in conjunction with:

- NPCC Alarms System Policy
- EN50131–1 Intruder Alarms Systems
- BS4737-1: Intruder Alarm Systems – Part 1: Specification for installed systems with local audible and/or remote signalling. (Withdrawn as a standard but still used for reference)
- EN50518:2019 Code of practice for remote monitoring centres
- BS9518:2021 Processing of alarm signals by an alarm receiving centre

- BS5979:2007 Code of practice for remote monitoring centres receiving signals for security systems.
- BS5839 Fire detection and alarm systems for buildings.
- BS EN 50131 (All parts), - Design and Installation of Intruder and Hold up Alarms
- BS EN 50136 (All parts), Alarm systems – Alarm transmission systems and equipment.
- BS8473 Code of practice for management of false alarms.
- PD6662 Scheme for the application of European standards for intruder alarm systems.
- BS8243 Systems designed to generate Confirmed Alarm conditions



Mission Statement

The company is committed to the continual development of all employees and to provide customers with an unrivalled level of products and service.



1.1 ARC/RVRC CONTACT INFORMATION

Southern Monitoring Services Ltd
Security House
212-218 London Road
Waterlooville
Hampshire
PO7 7AJ

Tel: 0844 871 2223
www.southernmonitoring.co.uk

The Team

General Manager

Stephen Lord 07580 790023
stephenl@southernmonitoring.co.uk

Customer Care Manager

Russ Lynas 07484 521532
rlynas@southernmonitoring.co.uk

Director of Operations

Chris Jones 02392 242 204
chrisj@southernmonitoring.co.uk

Administration Manager

Jack Hatfield 02392 242 301
jackh@southernmonitoring.co.uk

Operations Manager (SMS)

Stuart Lewis 02381 448623
stuartl@southernmonitoring.co.uk

Training Manager

Christina Cahill-Green 02392 242212
ccahill@southernmonitoring.co.uk

Operations

Engineer Priority Line

02392 242 043

Technical

Technical Help Line 02392 242334
Technical@southernmonitoring.co.uk

General Enquiries

Enquiries@southernmonitoring.co.uk

Credit Control

Credit Controller

Katie Peplow 023 9224 2244
creditc@southernmonitoring.co.uk

Team Mailboxes For Routine Transactions

Request type	Telephone	Email address
Data change	02392 242211	datachanges@southernmonitoring.co.uk
Dualcom	02392 242242	dualcom@southernmonitoring.co.uk
Redcare	02392 242235	redc@southernmonitoring.co.uk
Other system	02392 242205	applications@southernmonitoring.co.uk
Engineer ID	02392 242246	applications@southernmonitoring.co.uk
Deletions/reinstatements	02392 242235	deletions@southernmonitoring.co.uk
Billing	02392 242244	creditc@southernmonitoring.co.uk
General enquiry	02392 265114	enquiries@southernmonitoring.co.uk



1.2 Police Force policy requirements & Unique Reference Numbers (URN'S)

A monitored alarm system is dramatically more effective if the Police respond to alarm signals. Unfortunately, a considerable number of alarm signals from intruder alarm systems are false. We are dedicated to the task of reducing the number of false alarms significantly and to help you to conform to the Security Code of Practice for the Management of False Alarms.

It is the purpose of this section to inform you about the main requirements of the NPCC as they affect the user of an alarm system and our operational procedures.

We seek your co-operation to ensure that the Police requirements are fully understood and practised so your company remains on the Police list with a minimum of false alarms.

Note: Some police forces adopt variations on the national response procedures.

1.2.1 Your Alarm Systems

The Police require that intruder alarm systems are installed, maintained, and used in accordance with the current British Standards BS8418, BS8484, EN50131-1, PD6662, DD243 and BS8243.

1.2.2 Your Alarm Receiving Centre (ARC).

Alarm systems are monitored twenty-four hours a day by our Alarm Receiving Centres which conform to EN 50518 (Category I Alarm Receiving Centres) and we operate a RVRC conforming to BS8418. We operate a recognised Quality System for the monitoring of Intruder Alarms, Fire Alarms & Video monitoring to BS EN ISO 9001:2015.

1.2.3 Police Response

Police Response – the following information may vary from force to force. Police response will only

be given to:

- A burglary alarm (unconfirmed) from a system installed prior to October 2001.
- A confirmed alarm from any system installed/and or upgraded post October 2001.
- A video system conforming to BS8418.
- A lone worker alarm conforming to BS8484.

Unconfirmed alarms will only receive keyholder response (local variations may apply).

For confirmed alarm systems there are normally two levels of Police response.

LEVEL 1 - Immediate

LEVEL 3 - No Police attendance, keyholder response only.

The Police response to an alarm signal depends on the level the system is assigned and the individual Police Forces Standard of service.

Following 3 false signals in a rolling twelve-month period level 3 response is imposed and the Police will notify you of this in writing it is also your responsibility to notify the ARC/RVRC in writing on any change affecting the URN.

1.2.4 Alarm Systems with Personal Attack Devices

If the alarm includes a personal attack (PA) device, LEVEL 1 response to PA alarms will be maintained even after withdrawal of response to the intruder alarm. However, if after withdrawal of Police response, the PA element generates 3 more false signals in a rolling twelve-month period, response to PA alarms will also be withdrawn it is also your responsibility to notify the ARC/RVRC in writing on any change affecting the URN.

Note: Local variations apply in that some police forces adopt a strict 2 false alarms in a rolling 12-



month period whereby police response to a PA will be withdrawn irrespective of the alarm systems false alarm rate.

1.2.5 Action Following Withdrawal of Police Response

Police response to the alarm system will not be restored automatically and it is the responsibility of your customer to apply to the Chief Constable for restoration of response. The application should be supported by written evidence from the Alarm Company that the system has been free of any false alarms for a period of three months and that the system has been upgraded to alarm confirmation technology.

If withdrawal of Police response continues for more than six months the system will be deleted from Police records and it will be necessary to re-apply to the Police, through the alarm company for restoration of response.

1.2.6 Definition of a False Call

A false signal is an alarm signal, which would normally be passed to the Police and has not resulted from:

- a) Criminal attack or attempt of such, on the protected premises, the alarm equipment or the line carrying the alarm signal.
- b) Actions by the emergency services in the execution of their duty.
- c) A call emanating from a Personal Attack system made where has been a personal threat or attack on an individual.
- d) Activation of detectors without apparent damage, incorrect entry or exit to the premises and line faults will be considered as false alarms unless proved otherwise.

1.2.7 Confirmation of Alarm Calls

The alarm system must incorporate facilities to reduce false calls by confirming alarm activation. Correct use of such facilities is likely to attract continued LEVEL 1 response. However incorrect use

will result in LEVEL 3 response being imposed after 3 false calls in a rolling twelve-month period.

1.2.8 New Systems

Any alarm activations from new systems will not be passed to the Police unless it is a personal attack or a confirmed alarm, until fourteen consecutive trouble-free days of operation are achieved following connection to the ARC/RVRC, and with the proviso that we have been notified of the URN. It is the Alarm Company's responsibility to extend the 14-day test period where required.

1.2.9 Upgrading Systems to Confirmation

Existing Systems (E Event Codes)

The E prefix event Codes have been in use since September 1999 and these Event codes dictate the action taken on receipt of an alarm signal. E Event Codes are used for all systems installed prior to 1 October 2001.

Therefore, a system installed before 1 October 2001 (that has not lost Police response) but is upgraded to confirmation will be passed to the Police for unconfirmed, confirmed and com-fail alarms unless otherwise advised by the Alarm Company.

1.2.10 Existing Systems which have had Police Response Withdrawn

A system that has had Police response withdrawn will only qualify for reinstatement provided the system has been upgraded to confirmation technology compliant with BS8243.

All existing systems that have Police response reinstated will have Police response for P/A's & Confirmed Alarms only.

All existing systems that have Police response reinstated will have keyholder Notification only for Unconfirmed Alarms.

To ensure that you attract the correct response when police reinstatement occurs, please state that you wish for the system to be upgraded to confirmation with X Event codes. On receipt the administration department will upgrade the system



to confirmation and BS243 by changing the E event codes to X event codes.

1.2.11 Police Response / URN (Unique Reference Number)

For the Police to respond to an alarm activation, in most cases it is necessary for us to quote a URN (Unique Reference Number) when passing the call to the Police control room. All URN's are now issued direct to the Alarm Company by the Police authorities. URN's will only be issued where an alarm installer is a member of a recognised inspectorate.

1.3 GENERAL INFORMATION

1.3.1 Alarm Company Security Codes

All Alarm Companies should issue their Engineers and office staff with individual Company ID's using SMS Form "05:04 Company Security ID" and available on MASweb. Once completed simply email the form to our Administration Department. This will allow you to use MASweb to access your accounts remotely to place them on test, update keyholders, run reports etc. As part of the Sales Pack each Alarm Company will be issued with an Administration Company Identification Number (ID).

Note: Please ensure that engineers and office staff are aware of your Company Identity Code.

1.3.2 End User Security Codes

End Users will be required to quote a password or passcode as standard when calling into the ARC/RVRC by telephone unless otherwise agreed in writing.

Note: Please ensure that your customers are informed of their Account Number and Passcode.

1.3.3 Application Forms

To comply with our Quality System (BS EN ISO 9001:2015) all order requests for service must be made on an application smart form and we will aim to implement them within 24 hours of receipt Monday to Friday 08.30 – 17.00 excluding Bank Holidays.

If you require assistance to complete the form please contact the administration department who will be happy to help you.

Emergency requests for service for Digital Communicators only will be processed provided all critical data is supplied prior to the engineer attending site.

1.3.4 Instructing the ARC/RVRC

All instructions with a security implication should be made in writing to the Administration Department. we will aim to implement them within 24 hours of receipt Monday to Friday 08.30 – 17.00 excluding Bank Holidays.

Instructions can be accepted directly from End Users provided they are registered keyholders or users and can provide the necessary account and pass card number or word, unless otherwise directed by the Alarm Company.

Note: SMS & NMS do not accept liability for any loss or error that may occur as a result of:

a) Any instructions that have not been submitted via one of our approved Smartforms (available on MASweb).

b) Any instructions not submitted in writing by the Alarm Company in a word / email format.

c) Where the Alarm Company has not received a e-receipt of SMS & NMS communications relating to remote access data changes.

1.3.5 Visiting the ARC/RVRC

As you will appreciate the ARC/RVRC is a high security building and access is strictly controlled. No access to unauthorised persons can be permitted without a pre-arranged appointment and visitors must be accompanied within the building at all times.

The Alarm Receiving Centres do however encourage visitors and will be delighted to show interested individuals or groups the ARC/RVRC and provide a comprehensive tour.



1.4 APPLYING FOR AN ARC/RVRC CONNECTION & AMENDING CURRENT CONNECTION DETAILS

Southern Monitoring Services use Smartforms to add, amend or delete your accounts and are available from the Applications Tab on MASweb. The Smartforms are “live” only populating the required fields for the action you are carrying out and can be used on any device with internet access.

On Mas Web under the header ‘Application’ you will see a variety of different Smartform application forms available, this is due to the number of different systems we can accept and load onto our platform. If you are unsure which application form to use, then please contact the SMS Admin team who will be happy to help.

Under the header ‘Application’ you will also have access to the amendment form, this form is to be used to amend or update account information including keyholders, URN’s, Zones etc.

1.4.1 Digital Communicator

Complete the Other Systems Application Smartform and select the Digital Communicator option.

We will supply you with the correctly programmed chip (PROM/EPROM) if required (if you wish to undertake the programming of chips these will be supplied free of charge).

If the details are correct, you may attend site at your convenience to commission the alarm system and transmit test signals through to the ARC/RVRC.

1.4.2 Applications

Note: Some connections are billable from the date of enablement and no credits are given for the first 12 months of connection. For more information contact the SMS Admin team.

Orders that are submitted incorrectly will be rejected by email, which will indicate any discrepancies. Correct information must be re-submitted within 7 days. Failure to provide the information will initiate a second communication

indicating the discrepancy with a further 7 days to respond. No response within this period will result in the application being rejected and deleted.

Open / close is required on all intruder systems.

1.4.3 Upgrades

You can only upgrade using the relevant Smartform and selecting Re-grade, please answer all questions so the team know what type of request you are asking for.

1.4.4 Individual Transfers

It is essential that you should notify your existing ARC/RVRC of your intention to transfer system/s and the anticipated date, also please ensure that all financial accounts are up to date, otherwise they may delay transfer. Complete the relevant Smartform and select the Transfer In option.

You should arrange with your current ARC/RVRC to receive pro rata credits.

Open / close is required on all intruder systems.

We will inform you that the transfer is ready and upon receipt of authorisation from you the transfer will be carried out.

Note: A Transfer fee may apply.

1.4.5 Volume Connection Moves (VCM)

To simplify the transfer process with respect to existing connections, these can usually be transferred ‘on block’ at a mutually convenient time, negating the need to visit each site and change the chip.

A full customer data drop should be sent to our admin department, as this will be required to open the accounts in preparation for a block transfer. This is a report that can be obtained from your own database or from your current ARC/RVRC. When all the accounts have been opened a date is agreed for the transfer to take place.

Note: It is essential that you should notify your existing ARC/RVRC of your intention to transfer



systems to us and for you to have confirmation that all financial accounts are up to date otherwise the transfer may be delayed by the losing ARC/RVRC.

You should arrange with your current ARC/RVRC to receive pro rata credits for the unused portion of the year for each system.

On the day of transfer, the administration department will 'ID' all the accounts' to check their status and notify you of any anomalies

Note: A Transfer fee may apply.

1.4.6 CSL DUALCOM & EMIZON REGRADES

Within the first 12 months, regrading is not possible, unless upgrading under certain conditions.

Regrades for CSL Dualcom Pro range of products must be submitted via 'CHANGE GRADE' on CSL's My Base.

Regrades for CSL products (excluding Pro range) must be submitted by completing the CSL Dualcom Smartform application, selecting Regrade. Please answer all questions so the team know what type of request you are asking for. A regrade charge may be applicable.

For more information contact the SMS Admin team.

1.4.7 CSL DUALCOM & EMIZON DELETIONS

Deletions can only be submitted after the first 12 months.

For CSL Dualcom Pro range of products, deletions must be submitted via 'DISCONNECT SITE' on CSL's My Base.

For CSL products (excluding Pro range), deletions must be submitted by completing the Deletion / Suspension Smartform.

For CSL Routers, CSL will require the equipment to be returned. If you are unable to do this, charges may apply

1.4.8 AJAX OVERVIEW

Ajax Systems provide Wireless Smart Home security products to Installers around the UK.

The signalling paths are IP or GPRS, Video Verification is on our roadmap for introduction

The control Panels will send signals to MAS in SIA signalling. For further product information please visit: <https://ajax.systems/products/>

1.4.9 AJAX APPLICATION

The application can be found on MASweb under applications, then Ajax SmartForm.

When the order is received by SMS, an account for your customer is opened on our computer system and this will remain 'INACTIVE' until the system is commissioned

1.4.10 Remote Video Monitoring

The Remote Video Application Smart form can be found on MASweb under "Applications -> CCTV Application Form".

- Please indicate what CCTV Package and to what standard the system is compliant with.
- An account for your customer is opened on our Monitoring system and this will remain 'INACTIVE' until the system is commissioned.

Note: Systems requiring Police response must be installed to BS8418 and certificated.

1.4.11 Basic requirements for the System Design of a Remote Video System including RSI Systems

- Arming / Disarm of site to be controlled locally, either by an Access Control system, external proximity reader or keypads are acceptable means of setting the system. A schedule can be applied if this is not possible. A review of these timings must be in place to ensure suitable protection is met.
- Ensure that the system cannot be set off when the employee is entering/leaving site, eliminating any false alarms, that will require operator dispatch.
- Site to be protected must be a secure compound without covering any public rights



of way.

- Site must be secure of all loose items that could cause false alarms.
- Perimeter dual pair beaming to further reduce false alarms from animals and loose items should preferably be used to protect the site.
- Lighting levels should be high; locally this is a good deterrent and provides higher quality footage.
- All cameras must be in line of sight of detectors and preferably in colour.
- All cameras should cover one another for protection against masking.
- Consideration should be given to camera/detector coverage due to malicious blocking by stock items or high-sided vehicles if Redwall or similar detectors are deployed.
- Camera numbering must be in a logical sequence for monitoring of the site.
- System configuration should be that after receipt of an alarm activation further detection should alert the operator with new alarm pictures from the area concerned.
- Do not have standing instructions that may confuse the operator. Place filters that you want on the system locally at site by deploying correct system design. Allowing all alarms to signal to the ARC causes complacency as the site is always signalling to the operator and may cause dispatching delay.
- The object is only to transmit genuine pre-alarm trigger activation footage to the ARC.
- If PTZ cameras are used it is recommended that they are set to static when monitoring is active. This expedites operator response on trigger footage and allows our AI software to detect activity to support response.

- Any Pre-Alarm video sent to RVRC must contain at least 10 frames of video to allow of video verification to take place.

Commissioning

Before the system is made live, we undertake the following system checks:

- Resolution Acceptable
- Camera View / Closed Site
- Camera Descriptions
- False Alarm Check (Obvious Hazards)
- Schedules (Arming/Disarming)
- Audio Channels (If enabled)
- Firewall / Ports Check
- IP Address Static
- PTZ are 'static' during monitoring periods

We will also then check the Site address keyholders and any site-specific dispatch instructions.

Soak Testing

New Systems are strongly recommended to go on a 7-day soak test period where no action is taken on any activity, but incidents logged for installer review. This prevents keyholders being disturbed during the 'bedding in' period.

SMS Reserve the right to place system(s) on test without notice during the first 7 Days, if excessive / problems arise. Please ensure we have an isolation email address on file.

On BS8418 systems a sighting may result in contacting the authorities.

CCTV Alarm Dispatch

As standard we escalate incidents to keyholders when Person(s) / moving vehicle(s) are identified inside of the protected area. If the trigger image requires further investigation, a guard tour of nearby cameras will be undertaken. If the trigger alarm was due to weather / wildlife or unknown, then our action is to full clear the alarm noting any observations.

SMS Excessive Activation Policy

SMS have had much success with the monitoring of CCTV systems. However, we are



finding that due to the performance of some of the cameras/detectors that we are receiving excessive activity from certain devices due to several environmental factors such as sunlight, foliage or Staff / Authorised human activity.

The systems generally perform well, where installed according to the manufacturer's specifications. There are systems though where detectors have been placed in locations where they perform poorly, such as busy pedestrian areas or where they may be viewing large outdoor areas which they are not intended to do.

Each activation must be downloaded and viewed by our operators, and each false alarm detracts from the overall speed of response to what may be genuine incidents at other sites. SMS have a policy of identifying "rogue" detector/channels and removing these from operator action.

Where devices are identified, those which have signalled **3** or more times of up to 30 minutes (known as a runaway state), we will isolate the rogue camera /input/channel until it no longer falls within the above threshold.

Faulted Alarms

If a CCTV alarm is received where there is no associated video to be reviewed, then the alarm is cleared down with no further action taken.

Excessive Charges

SMS levy charges based on number of alarms above the site contract. As an example, a site on a CCTV**60** permit an average of 2 alarm calls per day.

Activations above 60 per Calendar month will be charged per activation.

We will always work with installers to negate these charges wherever possible.

AI Software

We use Artificial Intelligence software to reduce false alarms on CCTV installations. Please refer to the installer guide on the requirements, so that the software can perform efficiently. The software is set to fail safe and refer images to an operator if it

cannot decide. It is designed to detect moving vehicles and/or people unless specifically requested for persons only.

Minimum Camera Specifications

The effectiveness of the system is dependent upon certain configuration parameters. The Installer/Maintainer shall be responsible for ensuring the following configuration parameters are met:

- Camera Placement - Objects of Interest must not be blocked by other objects (e.g., trees, walls etc) and occupy at least 8% of the screen height and 10% of the screen width.
- The centre of a target object must move by at least 2% of the image width in a pair of consecutive images and still be completely visible in both of those images.
- For example, for a reference alarm containing images from a camera with a resolution of 320x240 pixels, minimum target object height and width is 25 pixels; and the object must move by 6 pixels in consecutive images.
- Camera Type: The Software currently supports images from a single lens camera only.
 - Images per alarm – minimum of 2 images per alarm.
 - Image Resolution:
 1. The resolution must have a minimum of 320x240 pixels for any security cameras.
 2. The resolution must have a minimum of 160x120 pixels for any RSI Videofied devices.
 - Image brightness - the average image brightness must be greater than 0.1 and less than 0.9; an individual pixel can take a value between 0 (black) and 1 (white).



1.5 COMMISSIONING AN ALARM SYSTEM

Commissioning a new account correctly is critical to ensure customer satisfaction and security. Before you connect the system, contact the ARC/RVRC and place the system on test informing the Operator that you are commissioning the system.

You will be asked for your Company I.D, the Customer's Account Number, Address, and the period you would like the system on test for. Ensure you have enough time to complete your work and do not exceed it as our software will automatically put the system back in service after the allowed time.

Activate each channel and note the order in which sent and in the case of dual signalling paths ensure that both paths are tested. This can be checked via MasMobile or an ARC Operator.

Contact the ARC/RVRC again and confirm receipt of the test signals. The operator, if required, can read back the signals received and make several checks to ensure the information we fold against the account is as required and complete. This is critical to ensure the correct response to each signal. It is important that the following information is correct; pins and responses, agency details, remote reset details, keyholder details, procedural instructions, and schedules if relevant. If all is correct tell the operator that you wish to commission the system – and the test can be cleared or left to 'time out'.

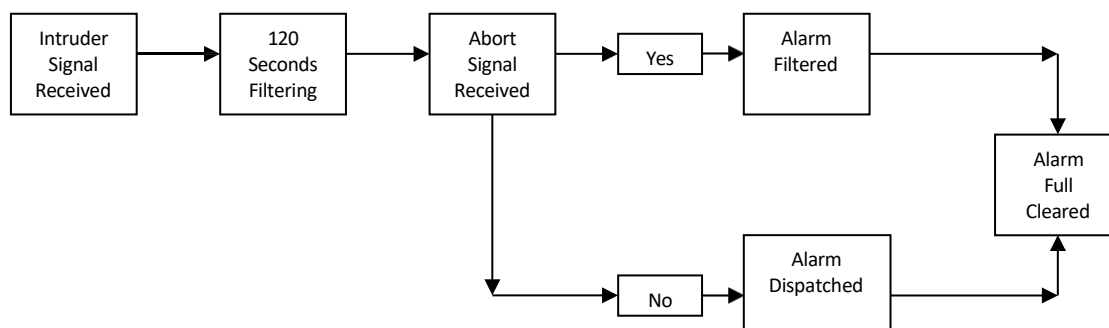
Before clearing the test or completing the process - Operator's will confirm with you if

the account requires a 14-day keyholder notification period with no Police response, in accordance with the NPCC Policy. When this is done commissioning is complete. Alarm systems will automatically go on to Policing after 14 days if a URN has been provided; it is the alarm company's responsibility to extend the 14-day test period where required.



1.6 ALARM RESPONSE

1.6.1 Automatic Filtering of False Alarms



If the alarm activates during setting or un-setting, the system must be turned off within one hundred and twenty seconds to automatically abort the activation. There is no need for the End User to ring the ARC/RVRC.

If the End User is under duress during setting or un-setting, turn off the system with the duress user code. This will ensure a silent duress 'Personal Attack' alarm message is received by the ARC/RVRC.

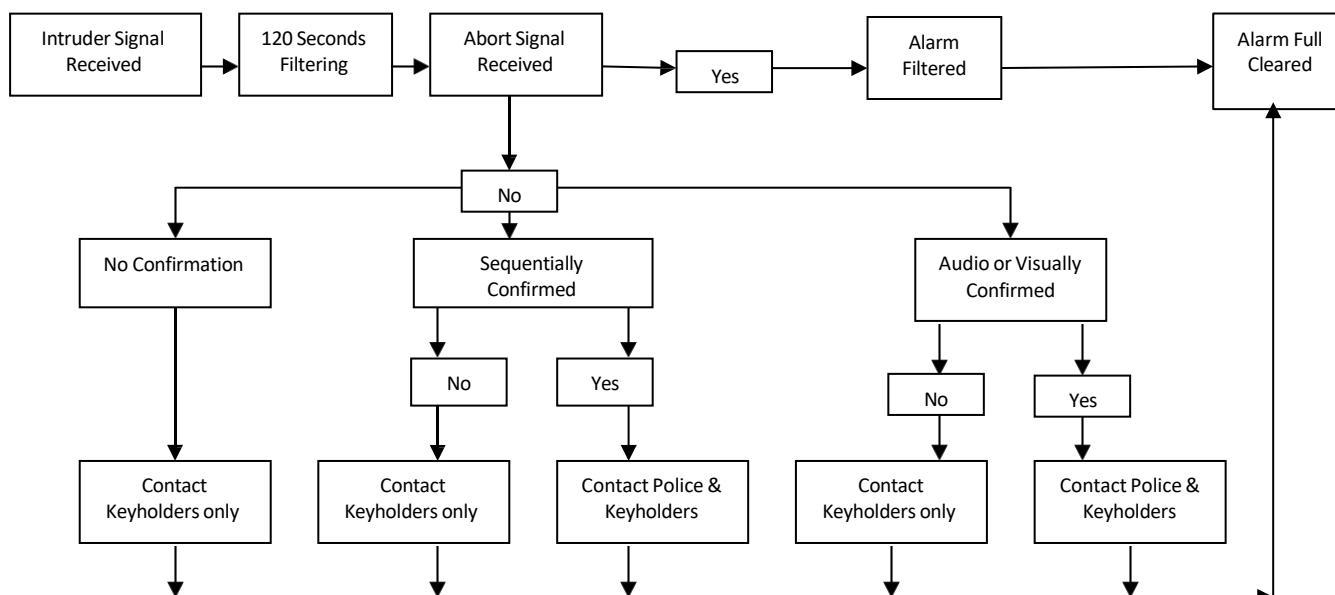
Alarm Confirmation

Alarm confirmation systems are mandatory for police response and are designed to reduce false alarms.

Note: Duress passwords are not accepted as a means of normal access to the ARC/RVRC for phone calls.

An activation of a Personal Attack button (or other deliberately operated device) at any time will result in a priority alarm actioned at your directive.

Alarm Filtering





BS8243

The above standard became mandatory from June 2012.

1) Tamperers - must be signalled as a distinct signal from Unconfirmed Intruder. A Tamper under BS8243:2010 + A1:2014 should be treated in the same manner as an Unconfirmed Intruder and therefore where received with either an Unconfirmed Intruder (within 45 minutes) or Unconfirmed Com Fail (within 96 hours in the same Set period) would be actioned as a Confirmed Alarm.

2) Confirmed PA Alarms - A BS8243:2010 + A1:2014 system will send a Pin 2 on PA (if in Fast Format) and this should be actioned to site/keyholders (or not at all) as an Unconfirmed PA. A second activation from the device will be signalled (if within 8 hours of the initial alarm) as a Confirmed PA on pin 7.

To achieve this all Alarm Installers must advise us on what standard the Alarm System is installed to on the Application Forms -

- | | |
|-----------------------|---------------|
| 1) BS4737/PreDD243 | E Event Codes |
| 2) DD243/PD6662:2004 | X Event Codes |
| 3) BS8243/PD6662:2010 | X Event Codes |
| 4) BS8243/PD6662:2017 | X Event Codes |

SMS & NMS do not allow the use of a "Generic" Confirmed on systems signalling in Fast Format. Where both a PA and an Intruder are being monitored on a system which is installed and accredited to BS8243 and using Fast Format the Pin 7 will be the Intruder Confirmation and another, different pin (Pin 1 for example if no Fire system connected) is to be used for PA Confirmation.

Tamper should be assigned an Event code of X6860 and our Operators will contact the Police where a Tamper & Unconfirmed Intruder signals have been received with 30 minutes (Intruder/Tamper) or 96 hours in the same Set period (Comfail & Tamper).

1.6.2 Alarm Confirmation Techniques - Sequential Confirmation

On receipt of an unconfirmed alarm signal at the

ARC/RVRC the automatic filtering procedures will apply. If after two minutes following receipt of the alarm signal no filtering has taken place the Keyholder will be informed of an 'Unconfirmed' alarm.

On receipt of a confirmed alarm if after a period of two minutes following receipt of the first alarm signal no filtering has taken place (unconfirmed restore or open signal) the alarm will be actioned as a "Confirmed Alarm" and the ARC/RVRC will inform the Police/Keyholders as required.

1.6.3 Alarm Confirmation Techniques - Audio Confirmation

The automatic filtering procedures will apply. If after a period of two minutes following receipt of the first alarm signal no filtering has taken place the ARC/RVRC Operator will listen for sounds of activity within the premises. If anything is heard the alarm will be actioned as an "Audio Confirmed Alarm" and the ARC/RVRC will inform the Police/Keyholders as required. If no sounds are heard a keyholder will be called.

1.6.4 Alarm Confirmation Techniques - Visual Confirmation

The automatic filtering procedures will apply, if after a period of two minutes following receipt of the first alarm no filtering has taken place the ARC/RVRC Operator will view images from the site, if these are consistent with an intrusion the alarm will be actioned as a "Visually Confirmed Alarm" and the ARC/RVRC will inform the Police/Keyholders as required. If images are not consistent with an intrusion a keyholder will be contacted.

1.6.5 Notifying the Police

If a URN has been provided, on receipt of an alarm signal, the call is passed to the appropriate Police Constabulary control room, the URN is quoted and an 'incident number' obtained.



The incident number, and the date and time the call was passed is entered into the computer system for record purposes.

1.6.6 Communication Failures

Unconfirmed Communication Failure

All signalling provider networks are susceptible to dropouts; therefore, all unconfirmed communication failures will be subject to a minimum filtering time of 60 minutes. This is to allow time for intermittent failures that affect signalling platforms to restore.

Where there is either a 'flood' condition or a known outage by way of communication from signalling / network provider we may place contingency measures in place to either clear down or extend filtering times to prevent unwanted disturbance to keyholders and provide service to high priority life alarms such as Fire, Panic Attack, Confirmed Intruder, etc.

When the alarm system is 'unset' and the ARC/RVRC receive an unconfirmed communications failure, this will NOT be passed to the Police.

Confirmed Communication Failure

When the system is 'set' and the ARC/RVRC receive a confirmed communications failure, a filter period of 60 seconds will apply. If communications are not restored within this time the ARC/RVRC will inform the Police/Keyholders as required advising them of a confirmed communications failure.

Communication failures received by the ARC/RVRC will be reported to the subscriber, keyholders and the Alarm Company. It is the Alarm Companies and the subscribers' responsibility to investigate the communication failure and effect repair.

Faults for RedCARE should be reported to British Telecom by ringing 0800 800151 for residential or 0800 800152 for commercial premises.

Faults for DualCom, Webway & Emizon should be reported to CSL technical Helpdesk on 01895 474 444.

For Redcare classic communication failures that have occurred because of power failure will require the STU being 'Upped'. This will only be done on authority of the Alarm Company to avoid substitute STU's being configured to a line.

Note: Prior to any action on receipt of a Redcare communication failure the operator will check to see if the ARC/RVRC has been notified by BT of expected failures due to maintenance work etc. In such circumstances and the site 'open' the operator will inform site or Keyholders and Alarm Company. If the site is 'closed' the operator will inform keyholder and alarm company.

Note: BT notified communication failures are not passed to the Police.

1.6.7 Redcare Link-down

A 'Link-down' is a condition that occurs when BT are working on the RedCARE Network. On receipt of a Link-down and the site is 'open' the operator will filter the condition for 30 minutes, if it has not restored within this time the operator will inform site or keyholder. If the site is 'closed' the operator will immediately inform a keyholder. Link-down conditions are not passed to the Police.

Phone Lines

Where alarm systems utilise phone lines, it is advisable for the alarm user to subscribe to the relevant support package with the phone provider to ensure 4-hour response in the event of a line fault.

1.6.8 Multiple Alarms

When multiple alarms are received, our Operators will handle these events in priority order. The highest priorities are Fire, Personal Attack, Confirmed Intruder and CCTV.

If multiple Intruder, Communication Failures and or Unconfirmed Tamper events are received, our Operators will check the Arm / Dis-arm status and will dispatch Agency if required.



1.6.9 Auto - Notification

As an Installer you can request to have an email notification set up for some alarm signals (known as "Auto-Notify") which will send an "Alarm Ticket" to the Keyholders for certain events.

Auto Notify can be used for any type of activation e.g.

- Fail to Open/Close
- Open/Close
- Industrial alarms
- Zone Omit
- Low battery
- Communication Failure
- Intruder
- Fire

If your customer wants, we can also action the alarm as normal and send an auto notification.

A further option is for alarms to be transmitted by SMS text. If this is the preferred method of notification to replace operator response, then there is no charge for this service. If it is addition to, then a nominal fee will be raised to cover network fees.

1.6.10 Alarm Automation (EVO)

Evo is a virtual operator that has been designed to pass alarms to Site / Keyholders. EVO uses the same phone number of 0844 0871 2223 so please advise your customers add as a contact in your phone's address book.

EVO will announce the following message: -

Hello, this is Southern Monitoring Services, we monitor the alarm at (Customer site Name, 1st line of the address, followed by Post Code). We have received (Alarm Type and Description) at (Time of Activation).

To accept responsibility of the alarm, the customer is invited to press 1 on their telephone, pressing 3 is instructing EVO to try another keyholder if there is one effectively declining to take responsibility. Pressing 7 will transfer you to an operator, If you

require any further information. Pressing 9 will repeat the entire message.

EVO is only applied to low priority alarms which are detailed below.

Fail-To-Test, Power Fail, Trouble, Industrial, Timed / Failed Schedule, Unconfirmed Intruder, Communication & Polling Fails, Zone Omit and Fire Fault.

We have a YouTube guide available through this link:

[EVO Operation - Guide](#)

1.6.11 ECHO

Southern Monitoring are fully ECHO connected in police force areas that offer a connection. ECHO is a not-for-profit organisation delivering automated alarm signalling and messaging between ARCs and blue light services, speeding up deployment of blue light responders to emergencies.

As a result of using ECHO police response is estimated (by ECHO) at 1-4 minutes quicker as a direct result of being ECHO-connected.

For more information on ECHO please see their website. <https://www.echo.uk.net>

1.7 PUTTING SYSTEMS ON OR OFF TEST

For servicing and maintenance of systems or whenever you are on site and require to "test" the alarm always ensure that the system is placed on test first to prevent unwanted attendance of the police or fire brigade. You can do this remotely using MASweb from your smartphone or Smart Test Plus from any mobile or landline, this service is operational 24 hours day, 7 days a week. For more information, please go to Section 2.

End Users requiring to take Personal Attack and Intruder Alarms out of service, can do so for up to a period of 8hrs (ID requirements must be satisfied).



There are various options available when remotely placing a system on test from being able to access single zones to placing the whole system on test from 30 minutes to 24 hours. For more information please contact us.

It is the responsibility of the person placing the system on test to ensure any signals sent are received at the ARC.

1.8 KEYHOLDERS

All monitored alarm systems should have at least two nominated keyholders unless a 24 hours keyholding service is utilised. A keyholder must be:

- A telephone subscriber.
- Have adequate means of transport to attend the protected premises at all hours.
- Must be capable of attending within twenty minutes of being notified.
- Have access to the premises.
- Have a good knowledge of the alarm system.

Should there be a change of keyholders, you are required to notify us within forty-eight hours. When calling keyholders the following standard procedure will be adopted: -

1.8.1 Initial Ringing of the Keyholder

The telephone will be allowed to ring for 30 seconds between 07:00-19:00 and 1 full minute at all other times; on successful contact the operator will advise the named keyholder of the alarm condition, we do not require a password/code at this time. If there is no response within 1 minute the operator will contact the next name on the list.

1.8.2 Engaged Line

The operator will try the number once, if

there is no response, they will move onto next keyholder, engaged lines may be tried again if no other Keyholder has been contacted.

1.8.3 Answering Machines

A brief message will be left asking the Keyholder to contact the ARC/RVRC. The operator will contact the next name on the list. Only one message is left with each Keyholder for an activation.

1.8.4 Unavailability of Keyholders

Agency Alarms

If no keyholders are available, the operator will advise the Agency that no keyholders are available.

Non-Agency Alarms

If no keyholders are available, we will advise the Installer / Maintainer by a report.

1.8.5 Keyholders

The Police require that any alarm activation from a system must be notified to a keyholder, previously nominated, and trained by you in the use of the alarm system. Following an activation, a keyholder will be requested to attend the protected premises to allow the Police to gain access.

Accounts with no listed Keyholders

Any account without Keyholders will remain "active" and in the event of an activation we will carry out the following:

1. If a Fire alarm activates and the account is on Agency response, we will pass the alarm in the normal manner.
2. If a Fire alarm activates and the account is on Keyholder response or 7/14/28 day test and we are unable to contact site, then we will pass the alarm to the Fire & Rescue Service.



3. If the Confirmed Burglary activates and the account is on Agency response, we will pass the alarm in the normal manner.

In all the above scenarios we will advise the agency there are no Keyholders available.

1.9 REMOTE RESETS

1.9.1 Operator Remote Reset.

The Remote Reset Service (where the facility exists) provides a means of resetting an alarm system, which has been activated without the need for alarm company attendance. A Remote Reset is only permissible when correct identification is given, the reason for the activation is clear and the false alarm rate for the individual system is not escalating.

The following Types of reset are available

Abacus	Pyronix	ADE
Regal Safe	Aritech	Risco
C K	Siemens SPC	Castle CareTech
SMS Reset	DSC	Technistore
Europlex	Texecom	FM
InnerRange	Scantronic	Menvier
Orisec	MDT	
SigNET	Guardall	Sintony

After the activation if the keyholder requests a reset, the operator will confirm the keyholders identity within the Alarm Companies requirements.

The operator will check the reason for the alarm activation and action as below: -

- Genuine Alarm - Reset to be denied unless authorised by the Alarm Company or engineer.
- False Alarm no apparent reason - Deny

Reset and refer to Alarm Company or engineer.

- False Alarm cause known - Check history for 2 previously Policed alarms, which has already been reset by a keyholder, over a 12 month period, if such history exists the reset will be denied on the basis that education or environmental issues need to be resolved.
- If all the necessary conditions can be fulfilled, reset action will take place. The operator will request the number displayed on the Remote Reset module from the keyholder on site.
- The operator will derive the anti-code.
- The operator will then give the keyholder the anti-code and ensure that the system control panel can be reset.
- All Remote Resets will be reported via the Remote Access System.

1.9.2 Engineer Remote Reset using MASweb

On MASweb you can download our engineer Remote Reset App. This is both for iOS and Android as well as PC / MacOS . This allows for reset codes to be generated.

By using MASweb it is also possible to record any Remote Resets so that it is recorded in Event History of the customer's file. These will be able to be reported on as requested.

2.0 GUIDE TO CO-ORDINATION AMENDMENTS

1. Navigate to <https://smonweb.co.uk>
2. Enter your normal Username and Password to login to your installer portal



Registered Users May Sign In Below

Login/SecUser:

Password:

- Click on the link called. "You have unread messages from SMS/NMS" as indicated below.

Welcome Chris

ACCOUNT STATISTICS OVERVIEW

# of Systems	Status
5	Total Systems Monitored
1	24 Hour Alarm Activity
0	Currently in Alarm Status
0	Systems Currently Open
0	Systems Currently Closed
0	Currently On Test
3	Out of Service
0	Systems with Pending Changes

[YOU HAVE UNREAD MESSAGES FROM SMS/NMS](#)

- On the next window click on the link called "Please select this link to access your Engineer Rota" as indicated below. If no link is presented, then please call technical support on 02392 242334 to have your login upgraded with your coordination link.

USER MESSAGE

[Please Select this link to access your Engineer Rota](#)

- The link should load your coordination file using Excel Online. At the bottom of the sheet click on the sheet named in black 'ALARM COMPANY ONLY'

Excel Online

Example Alarms (Servco 0000)

Please set the Coordination Times From 17:30 To 09:00 Current Date & Time 5/13/2015 07:17

TAKE THE FOLLOWING DETAILS :-

CALLERS NAME (Check Spelling)

CONTACT NUMBER (Ideally Landline)

SITE ADDRESS

POSTCODE

FULL DESCRIPTION OF THE PROBLEM / FAULT ON SITE

If the account is monitored, then has there been a policed activation?

Also advise of any activations on the account

- To make changes, click on the 'Edit in Browser' button. This allows changes to be made to the columns circled. The date is shown on the left-hand side to identify who will be on call that evening. Under the column "Closed" is where we would insert 'closed' such as bank holidays where you would want us to contact the duty engineer rather than pass calls to your office. (During office Hours) This may also be useful on days you wish us to take calls if your office was temporary out of action for any reason. Telephones upgrades, flood etc.

Excel Online

Example Alarms (Servco 0000)

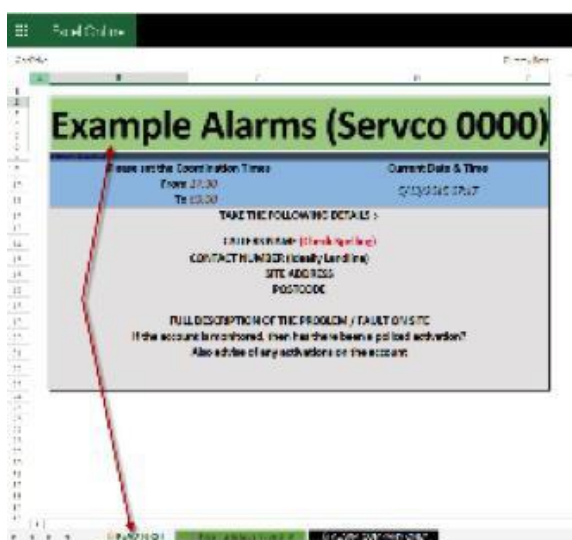
Date	Closed?	Day	Engineer Call List
5/12/2015		Thursday	Engineer Name A, Supervisor Name B, Manager Name C
5/13/2015		Friday	Engineer Name B, Supervisor Name C, Manager Name A
5/14/2015		Saturday	Engineer Name C, Supervisor Name A, Manager Name B
5/15/2015		Sunday	Engineer Name A, Supervisor Name D, Manager Name C
5/16/2015		Monday	Engineer Name B, Supervisor Name B, Manager Name A
5/17/2015		Tuesday	Engineer Name C, Supervisor Name C, Manager Name B
5/18/2015		Wednesday	Engineer Name A, Supervisor Name D, Manager Name C
5/19/2015		Thursday	Engineer Name B, Supervisor Name B, Manager Name A
5/20/2015		Friday	Engineer Name C, Supervisor Name C, Manager Name B
5/21/2015		Saturday	Engineer Name A, Supervisor Name D, Manager Name C
5/22/2015		Sunday	Engineer Name B, Supervisor Name B, Manager Name A
5/23/2015		Monday	Engineer Name C, Supervisor Name C, Manager Name B
5/24/2015		Tuesday	Engineer Name A, Supervisor Name D, Manager Name C
5/25/2015		Wednesday	Engineer Name B, Supervisor Name B, Manager Name A
5/26/2015		Thursday	Engineer Name C, Supervisor Name C, Manager Name B
5/27/2015		Friday	Engineer Name A, Supervisor Name D, Manager Name C
5/28/2015		Saturday	Engineer Name B, Supervisor Name B, Manager Name A
5/29/2015		Sunday	Engineer Name C, Supervisor Name C, Manager Name B
5/30/2015		Monday	Engineer Name A, Supervisor Name D, Manager Name C
5/31/2015		Tuesday	Engineer Name B, Supervisor Name B, Manager Name A

- Once the contents of a cell have been changed the document is auto saved ready to synchronise with our master local copy held for both SMS/NMS. Therefore, there is no actual 'save' button.

8. Once your changes have been made to exit politely for the next user, please click on the first sheet called 'READ FIRST' then click on the top green section with your company name, then close your browser down. This will effectively ensure the next time the coordination file is opened it reverts to the 1st sheet.

We only make available copies of these calls in accordance with the Data Protection Act to the parties recorded, the Police or due to court subpoena. Recordings are not for general release for the confirmation that a call took place, or that the information within that call was as stated. We do use some recorded calls internally as training tools and all calls are regularly monitored to ensure correct Business Telephone Practice is used by our staff.

Please note we are not permitted in accordance with the Data Protection Act 2018 to make available recordings of any conversations between parties to another third party unless it is in accordance with the procedure as stated above.



The screenshot shows a web browser window displaying a form titled "Example Alarms (Servco 0000)". The form has a green header bar with the title. Below the header, there are two columns: "Alarm and the Coordination Times" (From 17:30 To 18:00) and "Current Date & Time" (20/09/2024). The main body of the form is titled "TAKE THE FOLLOWING DETAILS:" and contains several fields: "USER NUMBER (if working on line)", "CONTACT NUMBER (usually Landline)", "SITE ADDRESS", and "POSTCODE". Below these fields is a section titled "FULL DESCRIPTION OF THE PROBLEM / FAULT ON SITE" with a sub-question: "If the alarm is monitored, then has there been a police activation? Also advise of any activations on the account." At the bottom of the form, there is a green button labeled "READ FIRST". A red arrow points from the "READ FIRST" button to the "TAKE THE FOLLOWING DETAILS:" section.

Section 2 Remote Access to the ARC/RVRC

Section 2:1

MASweb

MASweb. <https://www.smonweb.co.uk>

This is a portal where Installers can manage their sites and contact data, place accounts on test, read back signals etc. For an installer it is also the entry point to gain access to Smart Forms for applying for, adding to, and changing/deleting accounts. Once the installer enters their user name and password there are help videos posted on MASweb to guide them through basic procedures.

Section 2:1:1 MASweb Lite

MASweb. <https://www.smonweb.co.uk>

MASweb Lite is normally used by end users to place their fire alarms on test. Use the username and password provided by the installer follow instructions provided to place fire alarm on test and read back signals

2.2 DATA PROTECTION AND PRIVACY

The Police and/or the ARC/RVRC may hold any data supplied on computer. This data is subject to the Data Protection Act 2018, which is the UK's implementation of the General Data Protection regulation (GDPR).

SMS record all Telephone calls in and out of the business in accordance with Data Protection and Telecommunication Regulations. These calls are held in a secure BS EN 50518 ARC and are for protection of the business and our clients and you must ensure your employees, clients and their authorised keyholders are aware of this.



SECTION 2:1:2 MASMOBILE

MasMobile is an app for I Phone or android users and aimed predominately for engineers to use whilst in the field to place sites on and off test / read back signals. All details for settings etc can be found via MASweb or by contacting our tech department.

SECTION 2:2

Placing systems on Test using Smart Test

For end user carrying out fire alarm testing Smart Test + should be used.

For engineers, Smart Test+ enables them to use a 0800 FREEPHONE number and gives them more options when placing sites on test.

SMART Test+ Technician Instructions

How to place an account on test or get test results

1. Call freephone 0800 008 3045
2. Enter your Service Company number followed by '#'
3. Enter your Company ID number followed by '#'
4. Press '1' for the account menu.
5. Enter the Customer Account number followed by '#'
6. Follow the audio instructions to place system(s) on test or to read back signals sent and to clear the test.
7. If placing the account on test, enter category then press '#':

Cat 10 = 1 Hr	Cat 13 = 4 Hrs
Cat 11 = 2 Hrs	Cat 14 = 6 Hrs
Cat 12 = 3 Hrs	Cat 15 = 8 Hrs



Privacy Policy

As a subsidiary of Securitas, SMS adhere to the Securitas global privacy policy which is available here:

<https://www.securitas.com/en/about-us/securitas-technology-and-healthcare-global-privacy-policy/>

To comply with the Data Protection Act 2018 and the policy referenced above, there must be a lawful basis for us to collect, process and store any personal data that you provide us with. For Customers of SMS, the contract with yourself for the provision of Alarm Monitoring provides this basis, including but not limited to fault reporting and access to services, such as our web portal.

For your information, the data provided by you that we hold includes, but is not limited to, the following:

Company information of SMS/NMS Customers and End-users

Name, address and contact details; legal ownership and registration details; trading premises; company background; company activity; opening hours; supporting evidence.

Contact information of Customers and End-Users

Contact name, job title, business/residential address, business/residential phone number/mobile number/email address.

Other

Call recordings, alarm and activity logs and CCTV footage of customers or end-users through monitoring contracts with SMS.

We need to store this information so we can work with you throughout the duration of the contract and undertake activities such as alarm handling, out of hours co-ordination, debt collection, answering queries and complaints and the purposes of identification verification.

All information gathered is retained confidentially by SMS throughout the lifetime of the approval and then for the minimum legal requirement thereafter or as long as is required. We may be asked to disclose your information without your consent if we are required to comply with a legal obligation (such as a criminal investigation).

We know the issues of privacy and security matter to you as a customer and rank high in terms of your vendor selection criteria.

We act as a data processor for our customers (alarm companies) who we regard as data controllers.

If you have any questions about the information that SMS is required to hold, wish to request access or changes to your data, or your customer requires the same, please contact gdpr@southernmonitoring.co.uk

Our website

Important Legal Information

<https://www.smon.co.uk/terms-and-conditions>